QoS Best Practices

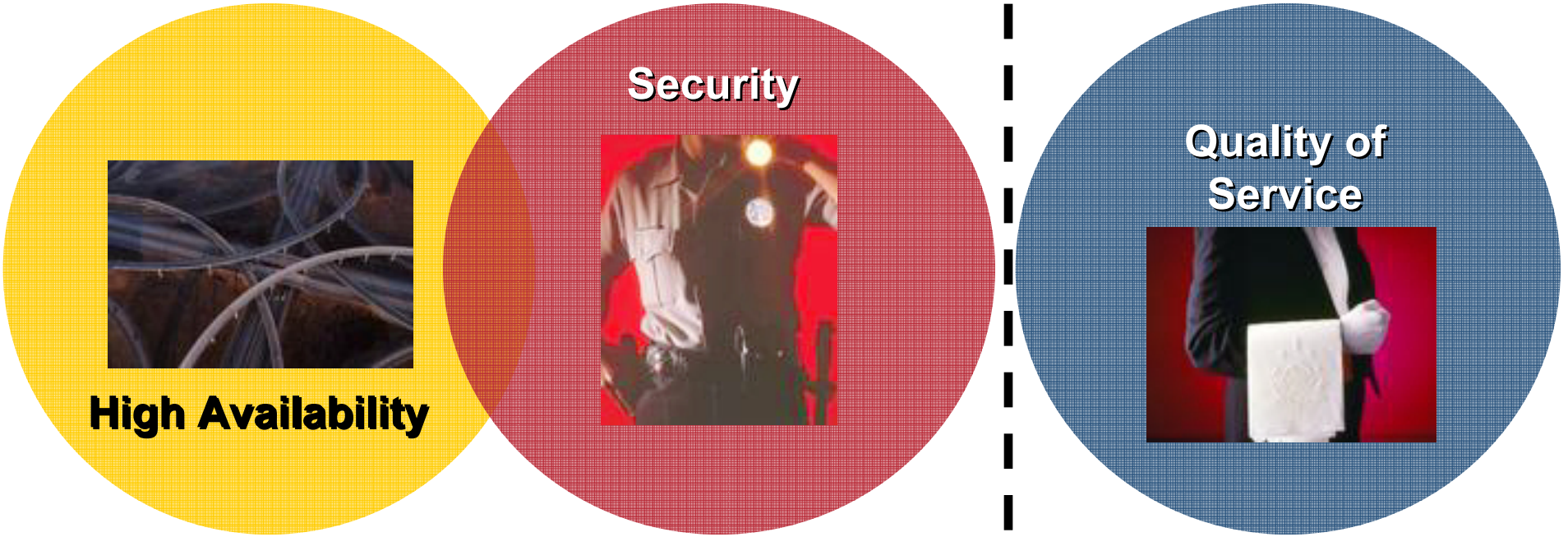
Tim Szigeti
Technical Marketing Engineer
Technology and Systems Marketing: QoS
Cisco Central Development Organization
10/5/04

QoS Perception

Changing the Way Intelligent Services Are Enabled

Cisco.com

Necessity | **Luxury**



QoS Deployment Principles

How is QoS Optimally Deployed in the Enterprise?

1) Strategically define the business objectives to be achieved via QoS.

2) Analyze the service-level requirements of the various traffic classes to be provisioned for.

3) Design and test the QoS policies prior to production-network rollout.

4) Roll-out the tested QoS designs to the production-network in phases, during scheduled downtime.

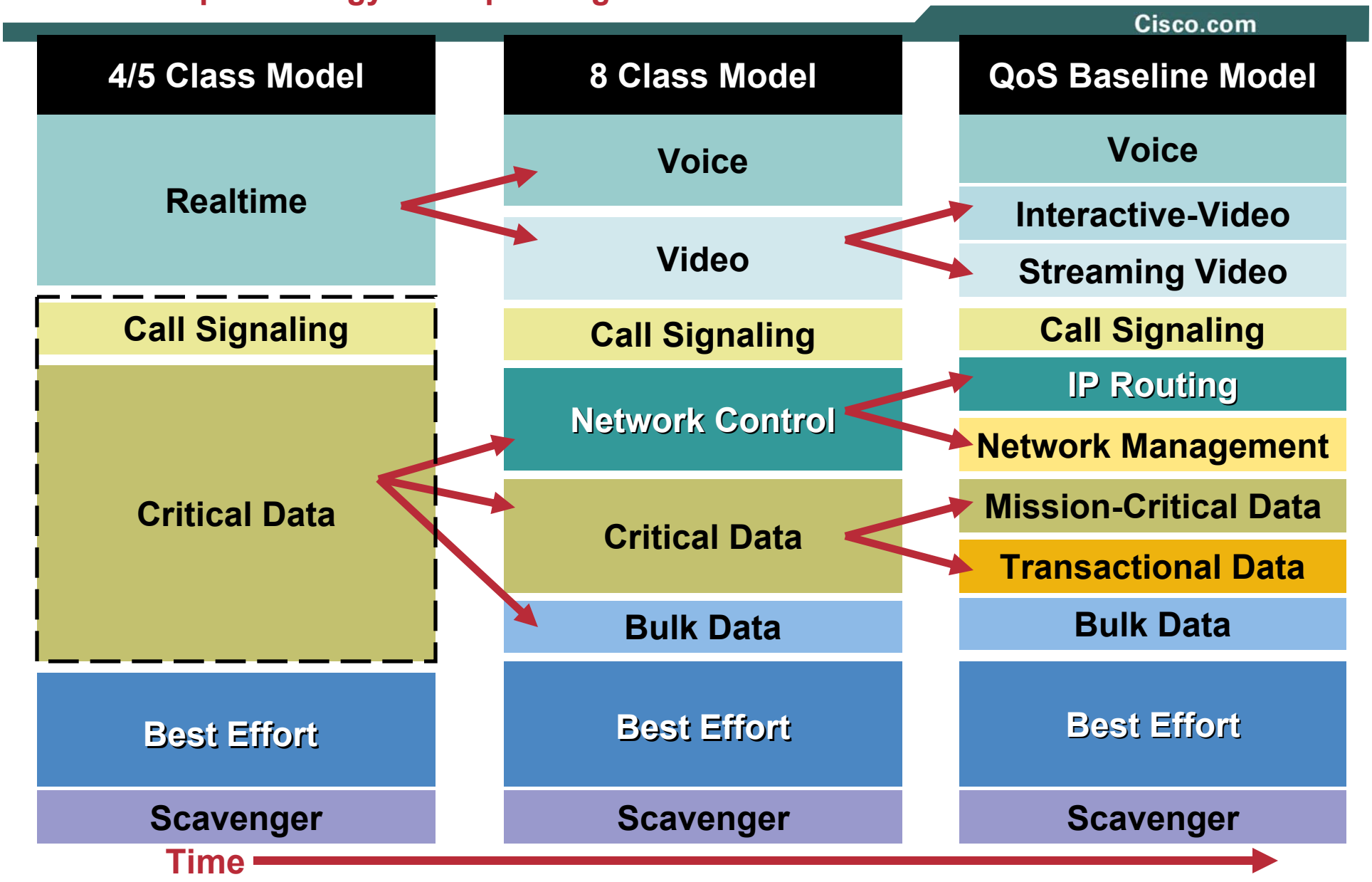
5) Monitor service levels to ensure that the QoS objectives are being met.

General QoS Design Principles
Start with the Objectives: Not the Tools

- Clearly define the organizational objectives
  - Protect voice? video? data? DoS/worm mitigation?
- Assign as few applications as possible to be treated as “mission-critical”
- Seek executive endorsement of the QoS objectives prior to design and deployment
- Determine how many classes of traffic are required to meet the organizational objectives
  - More classes = more granular service-guarantees

How Many Classes of Service Do I Need?

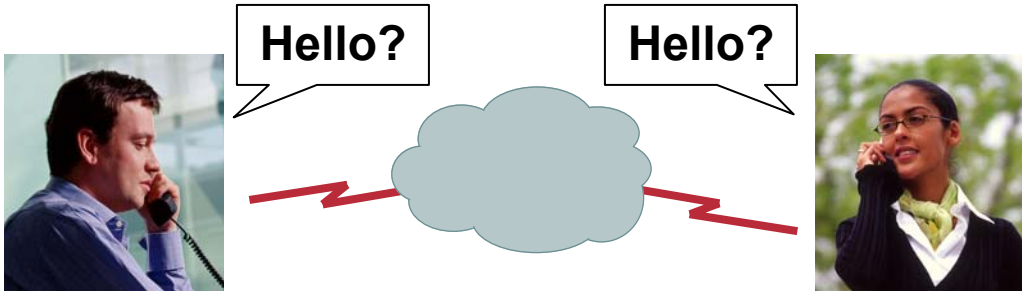
Example Strategy for Expanding the Number of Classes of Service over Time

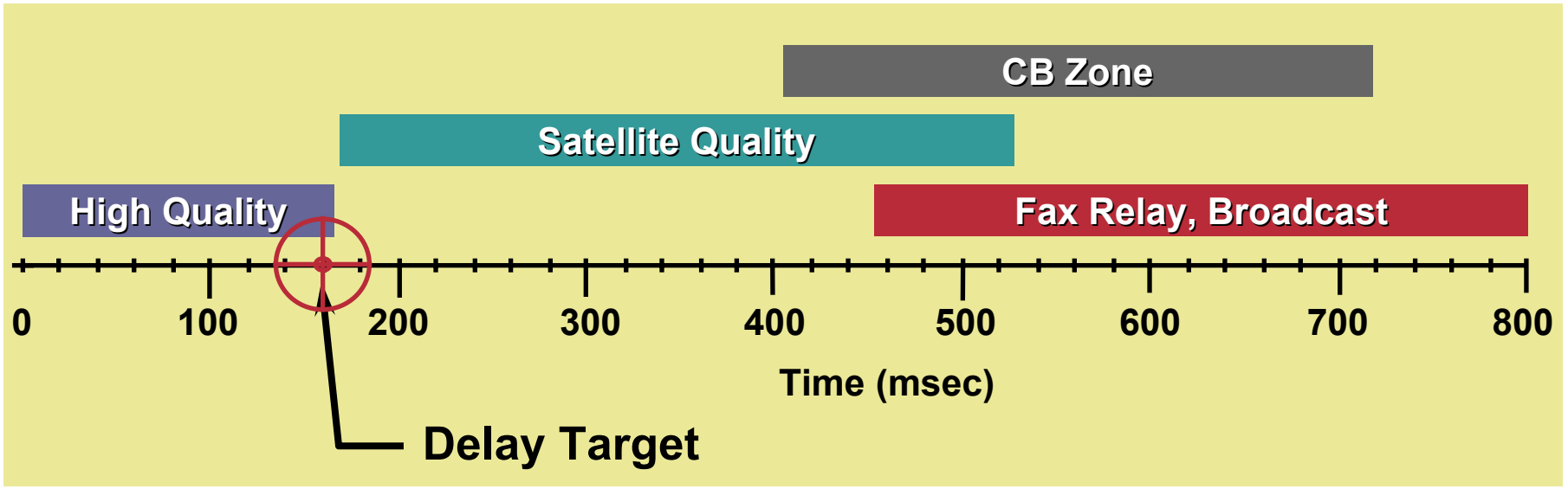


QOS REQUIREMENTS OF VOICE, VIDEO, AND DATA

Voice QoS Requirements
End-to-End Latency

Avoid the "Human Ethernet"



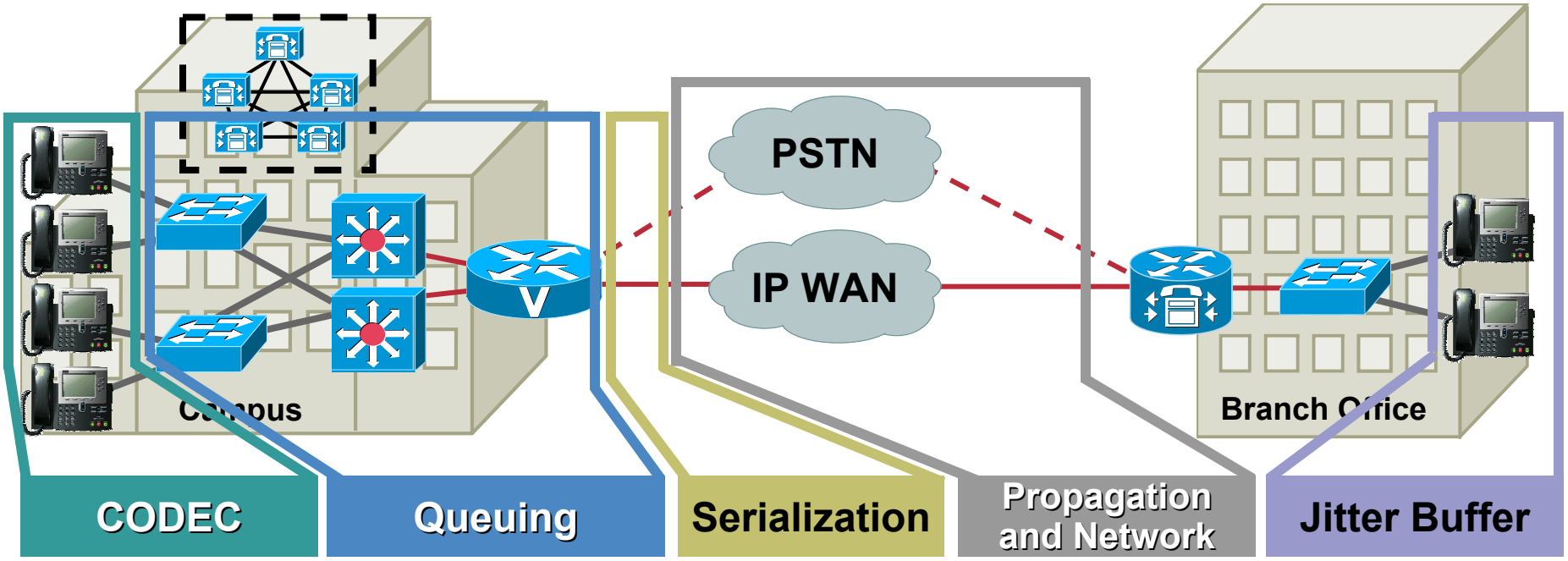


ITU's G.114 Recommendation: ≤ 150msec One-Way Delay

Voice QoS Requirements

Elements That Affect Latency and Jitter

Cisco.com

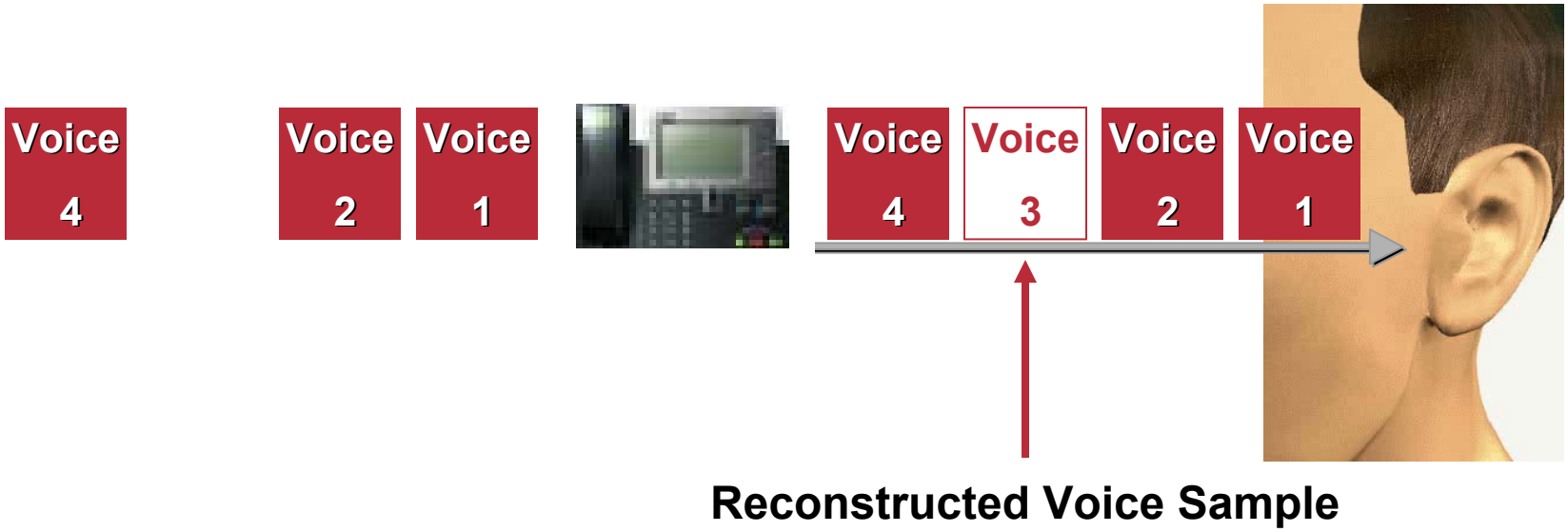


CODEC	Queuing	Serialization	Propagation and Network	Jitter Buffer
G.729A: 25 ms	Variable	Variable	Fixed (6.3 µs/Km) + Network Delay (Variable)	20–50 ms

End-to-End Delay (Must Be ≤ 150 ms)

Voice QoS Requirements
Packet Loss Limitations

Cisco.com

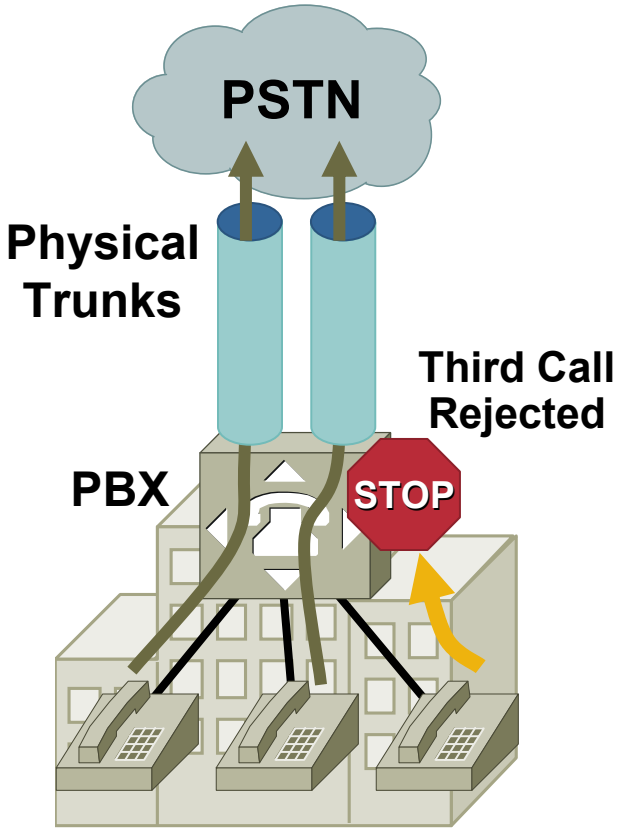


- Cisco DSP codecs can use predictor algorithms to compensate for a single lost packet in a row
- Two lost packets in a row will cause an audible clip in the conversation

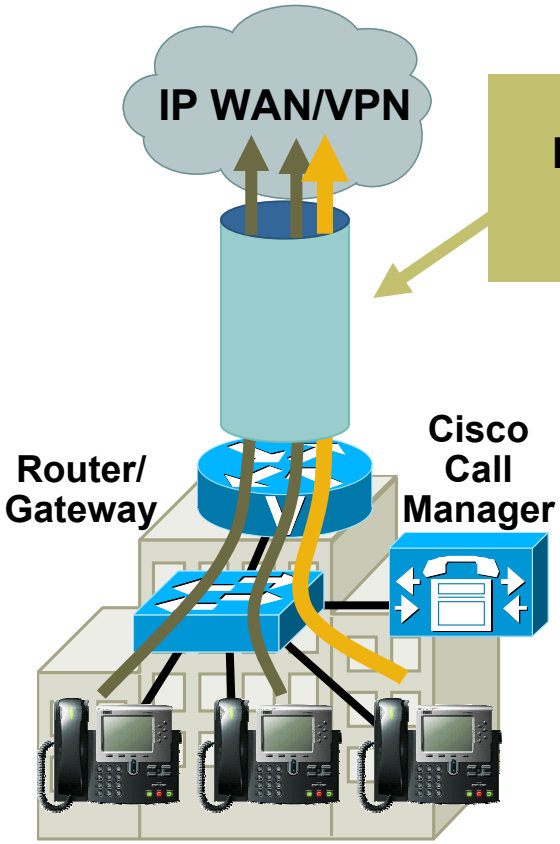
Voice QoS Requirements

Call Admission Control (CAC): Why Is It Needed?

Circuit-Switched Networks



Packet-Switched Networks



IP VPN Link Provisioned for 2 VoIP Calls

No Physical Limitation on IP Links

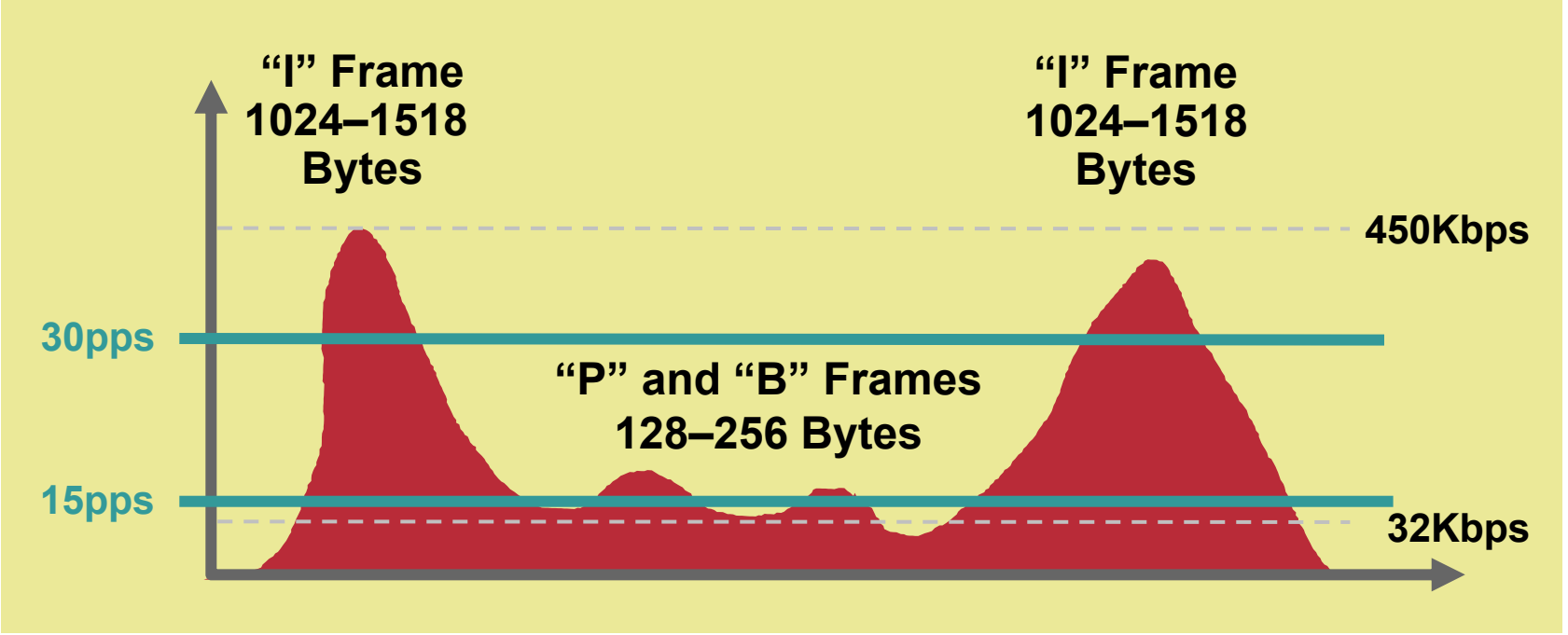
If 3rd Call Accepted, Voice Quality of All Calls Degrades

CAC Limits Number of VoIP Calls on Each VPN Link

Video QoS Requirements

Video Conferencing Traffic Example (384 kbps)

Cisco.com

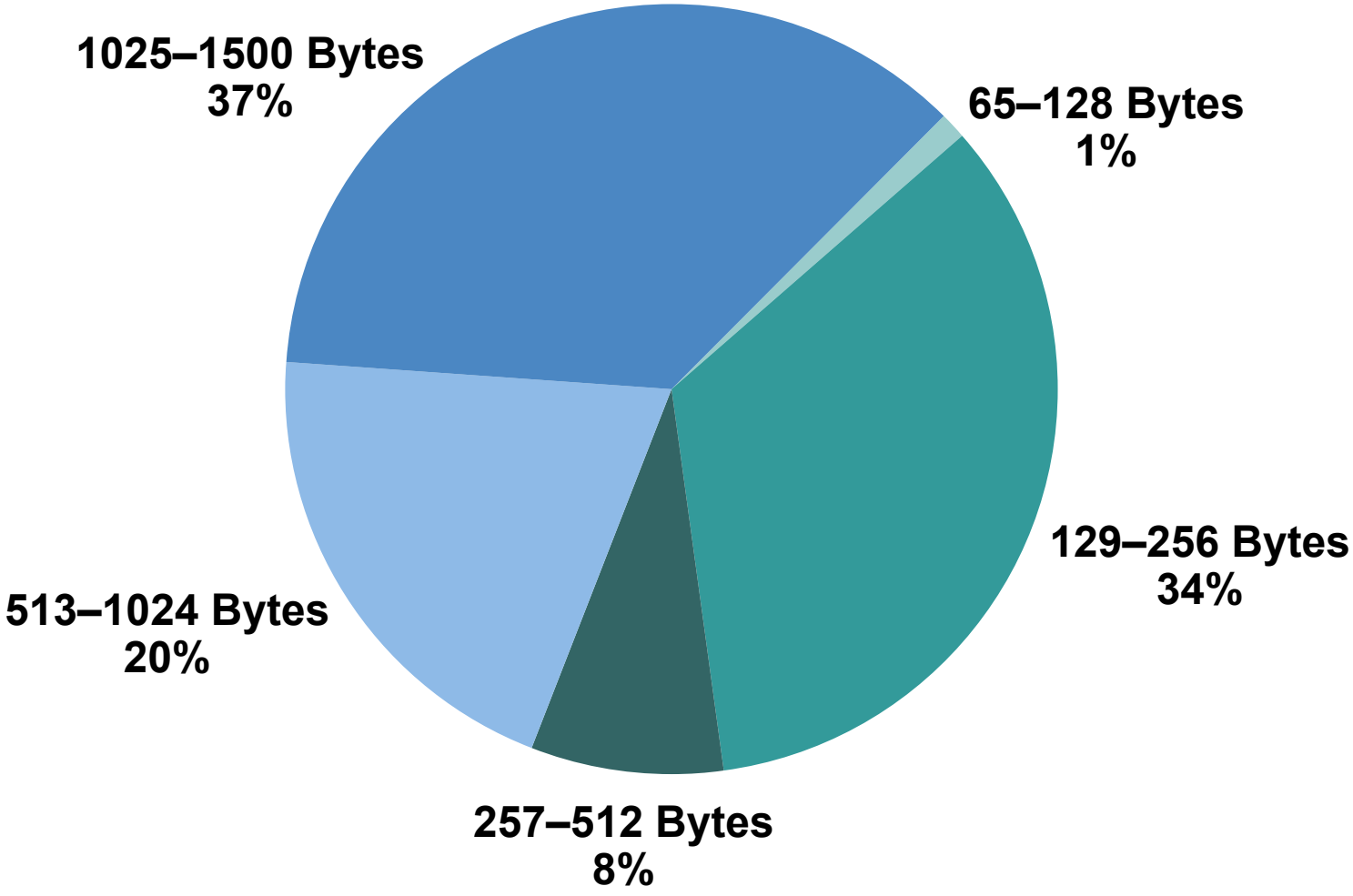


- "I" frame is a full sample of the video
- "P" and "B" frames use quantization via motion vectors and prediction algorithms

Video QoS Requirements

Video Conferencing Traffic Packet Size Breakdown

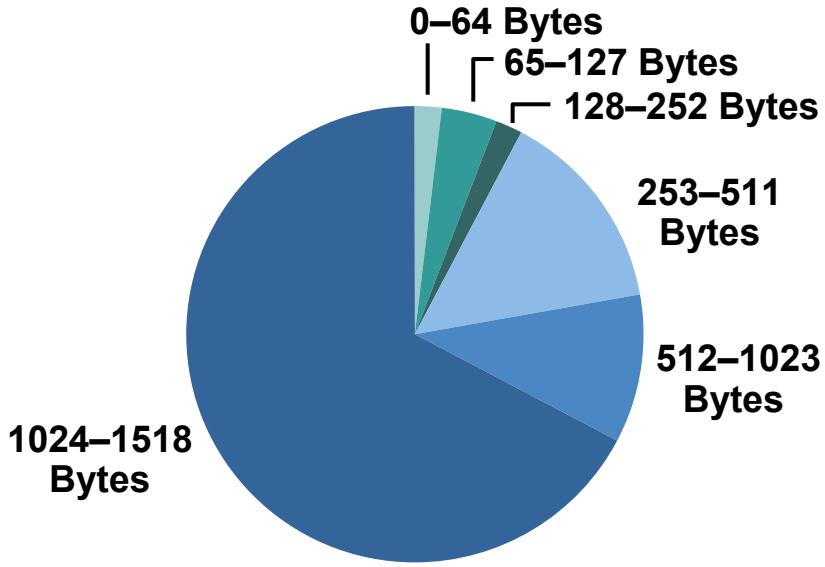
Cisco.com



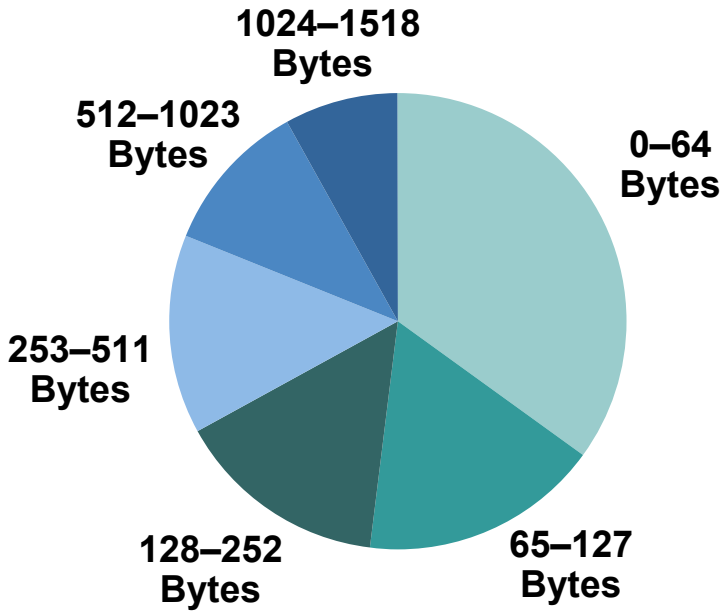
Data QoS Requirements
Application Differences

Cisco.com

Oracle



SAP R/3



Data QoS Requirements
Version Differences

Cisco.com

SAP Sales Order Entry Transaction

Client Version	VA01 # of Bytes
SAP GUI Release 3.0 F	14,000
SAP GUI Release 4.6C, No Cache	57,000
SAP GUI Release 4.6C, with Cache	33,000
SAP GUI for HTML, Release 4.6C	490,000

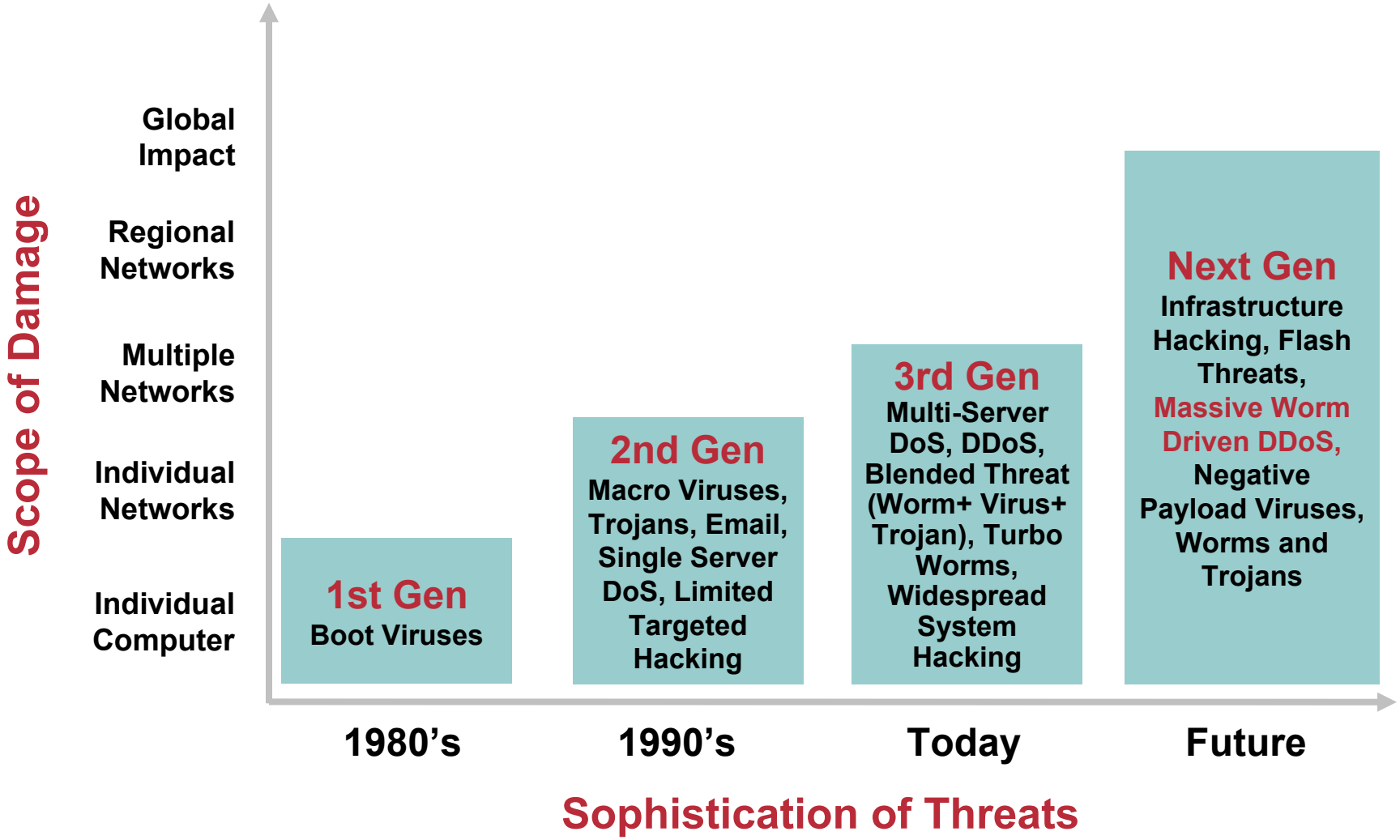
- **Same transaction takes over 35 times more traffic from one version of an application to another**

OVERVIEW OF DOS/WORM ATTACKS

Business Security Threat Evolution

Expanding Scope of Theft and Disruption

Cisco.com



Emerging Speed of Network Attacks

Do You Have Time To React?

Cisco.com

1980s-1990s
Usually had Weeks or Months to Put Defense in Place

2000-2002
Attacks Progressed Over Hours, Time to Assess Danger and Impact; Time to Implement Defense

2003-Future
Attacks Progress on the Timeline of Seconds

SQL Slammer Worm:
Doubled Every 8.5 Seconds
After 3 Min: 55M Scans/Sec
1Gb Link Is Saturated After One Minute

In Half the Time It Took to Read This Slide, Your Network and All of Your Applications Would Have Become Unreachable

SQL Slammer Was A Warning, Newer "Flash" Worms Are Exponentially Faster

“Slammer” or the Sapphire Worm

Infected 75,000 Hosts in First 11 Minutes

- Infections doubled every 8.5 seconds
- Infected 75,000 hosts in first 11 minutes
- Caused network outages, cancelled airline flights and ATM failures

At Peak, Scanned 55 Million Hosts per Second

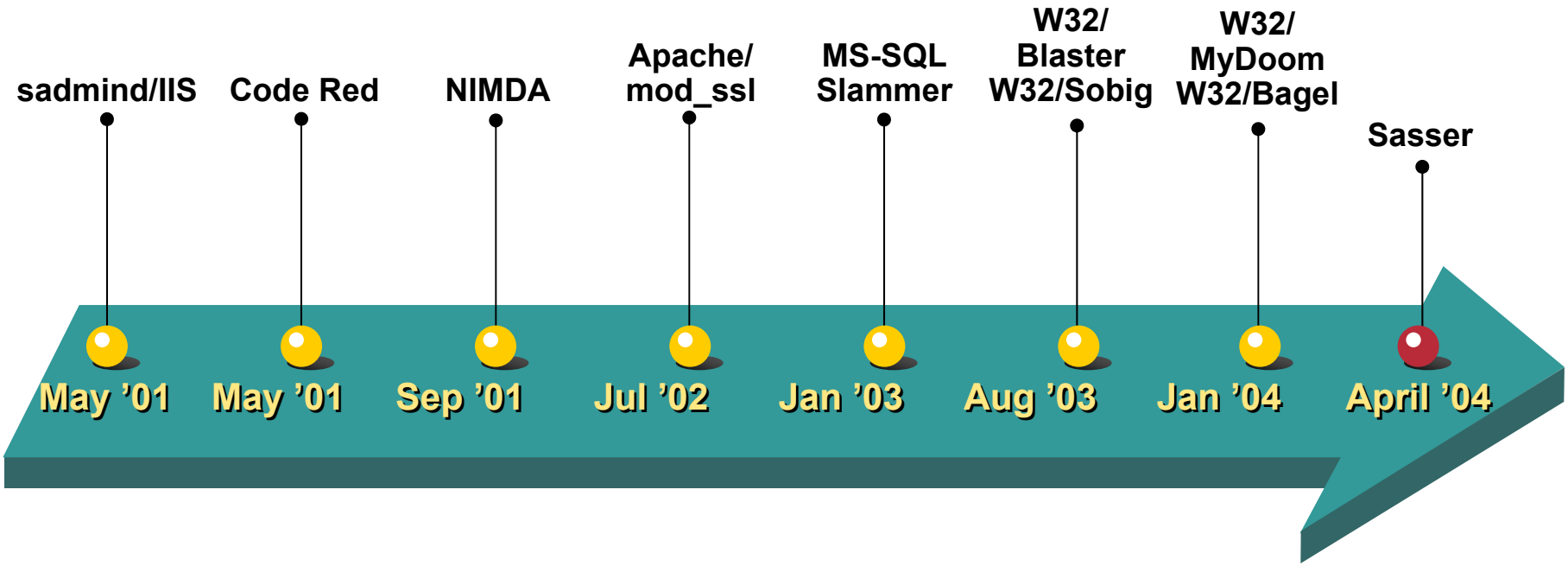
11 Minutes after Release

11 8 6 2 0

Internet Worms

By the Time You Read This Slide It Will Be Out of Date

Cisco.com



- More than 994 new Win32 viruses and worms were documented in the first half of 2003, more than double the 445 documented in the first half of 2002

http://www.symantec.com/press/2003/n031001.html

Types of DoS Attacks
Spoofing vs. Slamming

Cisco.com

- **Imposter attack**

  Pretends to be a legitimate service but maliciously intercepts/misdirects client requests

- **Flooding attack**

  Exponentially generates and propagates traffic until service resources (servers and/or network) are overwhelmed

Impact of an Internet Worm

Anatomy of a Worm: Why It Hurts

Cisco.com

1—The Enabling Vulnerability

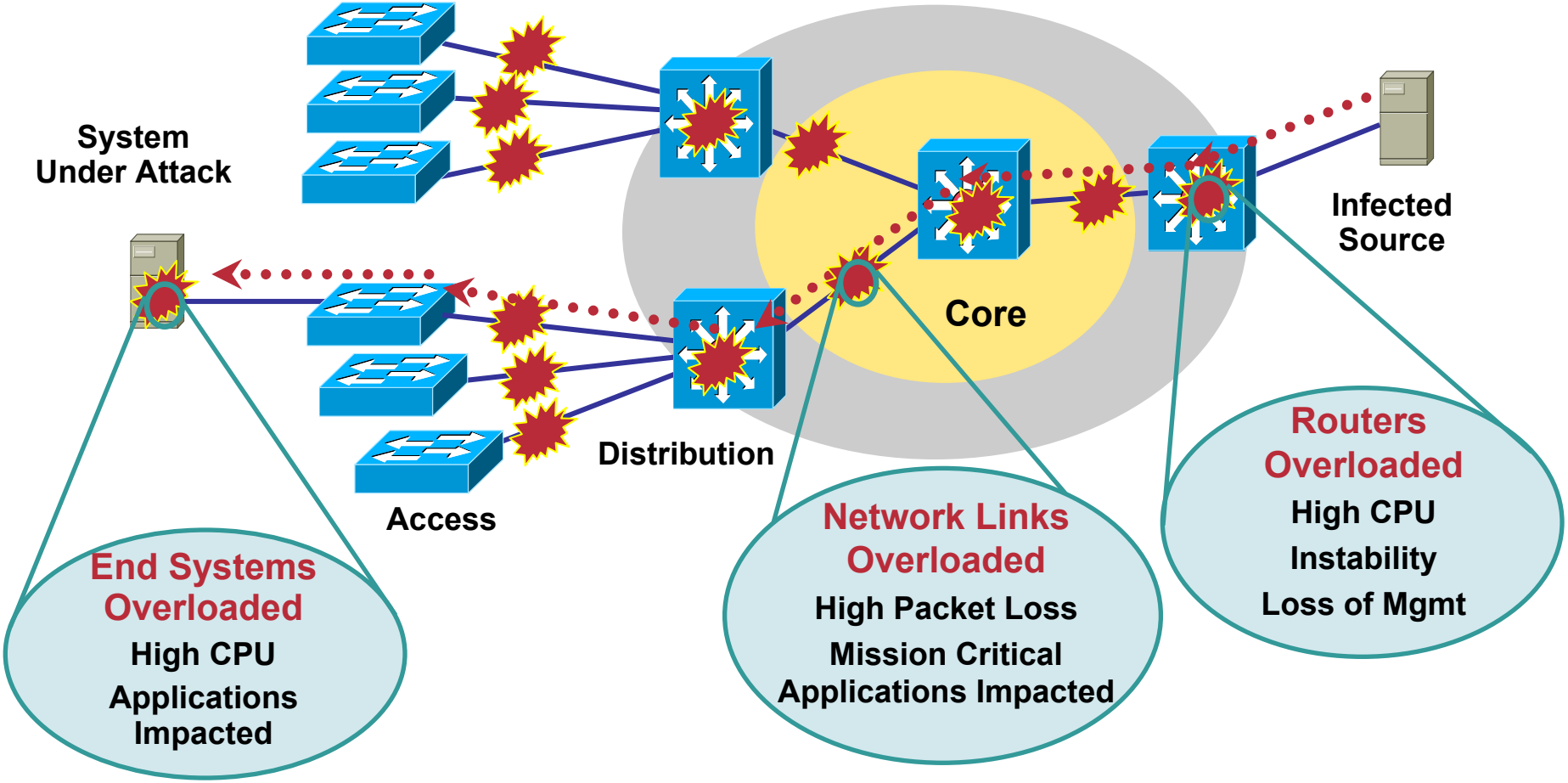
2—Propagation Mechanism

3—Payload

Impact of an Internet Worm

Direct and Collateral Damage

Cisco.com



Attacks Targeted to End Systems CAN and DO Affect the Infrastructure

QoS Technologies Review

QoS Technologies Review

Cisco.com

- QoS Overview
- Classification Tools
- Scheduling Tools
- Policing and Shaping Tools
- Link-Specific Tools

QoS Factors

Attributes Requiring Explicit Service Levels

Cisco.com

Quality of Service Operations
How Do QoS Tools Work?

Cisco.com

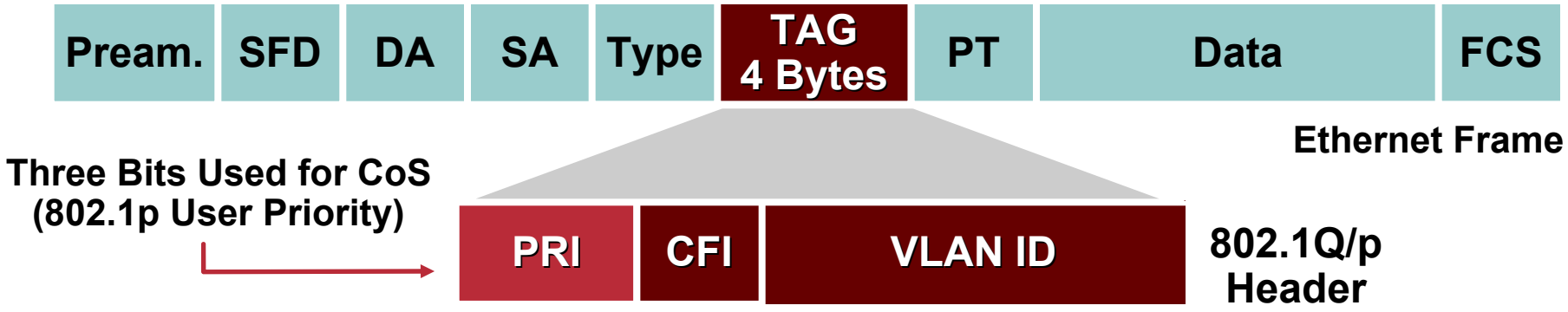
CLASSIFICATION AND MARKING

QUEUEING AND
(SELECTIVE) DROPPING

SHAPING/COMPRESSION/
FRAGMENTATION/INTERLEAVE

Classification Tools
Ethernet 802.1Q Class of Service

Cisco.com

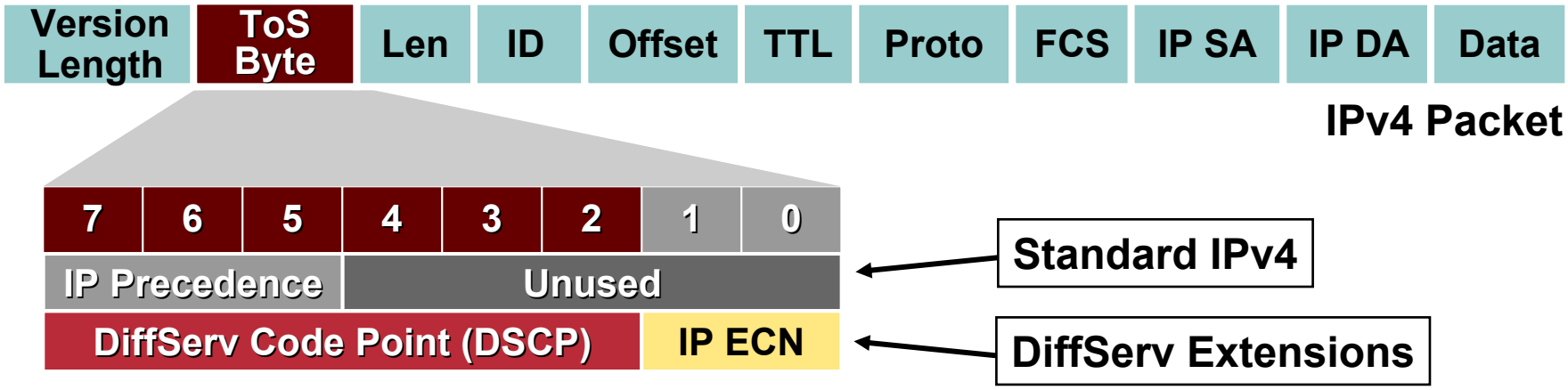


- 802.1p user priority field also called Class of Service (CoS)
- Different types of traffic are assigned different CoS values
- CoS 6 and 7 are reserved for network use

CoS	Application
7	Reserved
6	Routing
5	Voice
4	Video
3	Call Signaling
2	Critical Data
1	Bulk Data
0	Best Effort Data

Classification Tools
IP Precedence and DiffServ Code Points

Cisco.com



- **IPv4: Three most significant bits of ToS byte are called IP Precedence (IPP)—other bits unused**
- **DiffServ: Six most significant bits of ToS byte are called DiffServ Code Point (DSCP)—remaining two bits used for flow control**
- **DSCP is backward-compatible with IP precedence**

Classification Tools
DSCP Per-Hop Behaviors

- IETF RFCs have defined special keywords, called Per-Hop Behaviors, for specific DSCP markings
- EF: Expedited Forwarding (RFC3246, formerly RFC2598)

  (DSCP 46)
- CSx: Class Selector (RFC2474)

  Where x corresponds to the IP Precedence value (1-7)

  (DSCP 8, 16, 24, 32, 40, 48, 56)
- AFxy: Assured Forwarding (RFC2597)

  Where x corresponds to the IP Precedence value (only 1-4 are used for AF Classes)

  And y corresponds to the Drop Preference value (either 1 or 2 or 3)

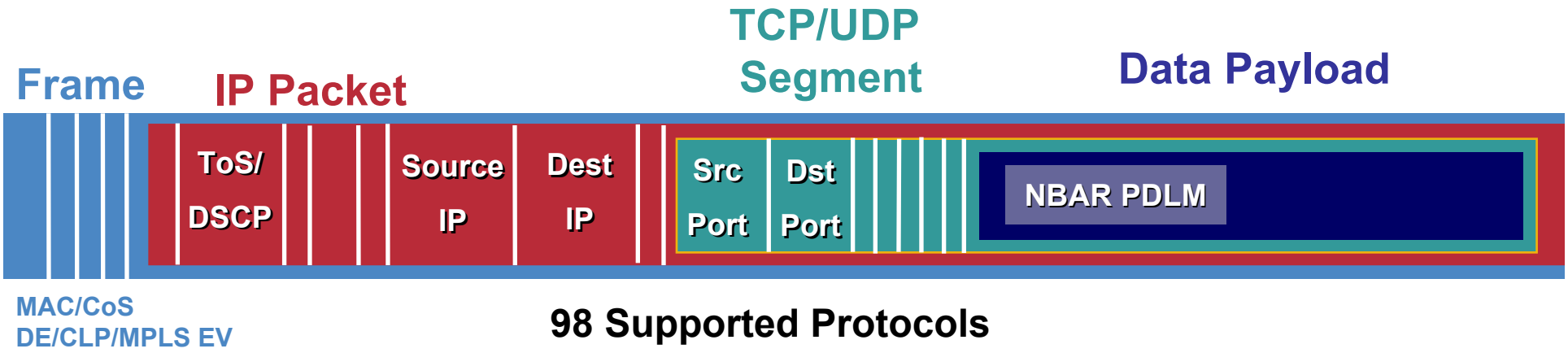
  With the higher values denoting higher likelihood of dropping

  (DSCP 10/12/14, 18/20/22, 26/28/30, 34/36/38)
- BE: Best Effort or Default Marking Value (RFC2474)

  (DSCP 0)

Classification Tools
Network-Based Application Recognition

Cisco.com

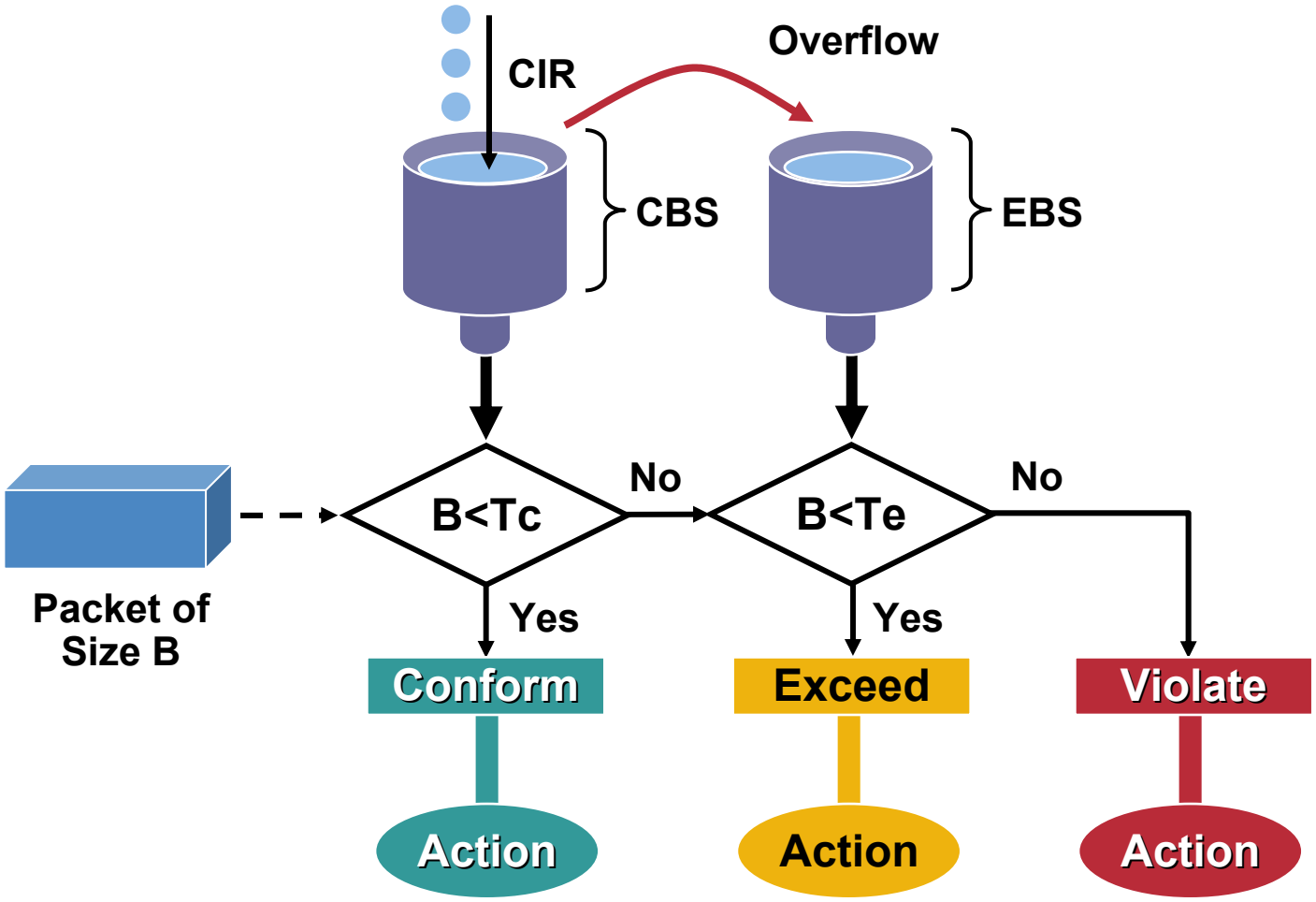


98 Supported Protocols

citrix	http	nntp	ssh	streamwork
cuseeme	imap	notes	smtp	syslog
custom	irc	novadigm	snmp	telnet
exchange	kerberos	pcanywhere	socks	secure-telnet
fasttrack	ldap	pop3	sqlserver	tftp
ftp	napster	realaudio	sqlnet	vdolive
gnutella	netshow	rcmd	sunrpc	xwindows

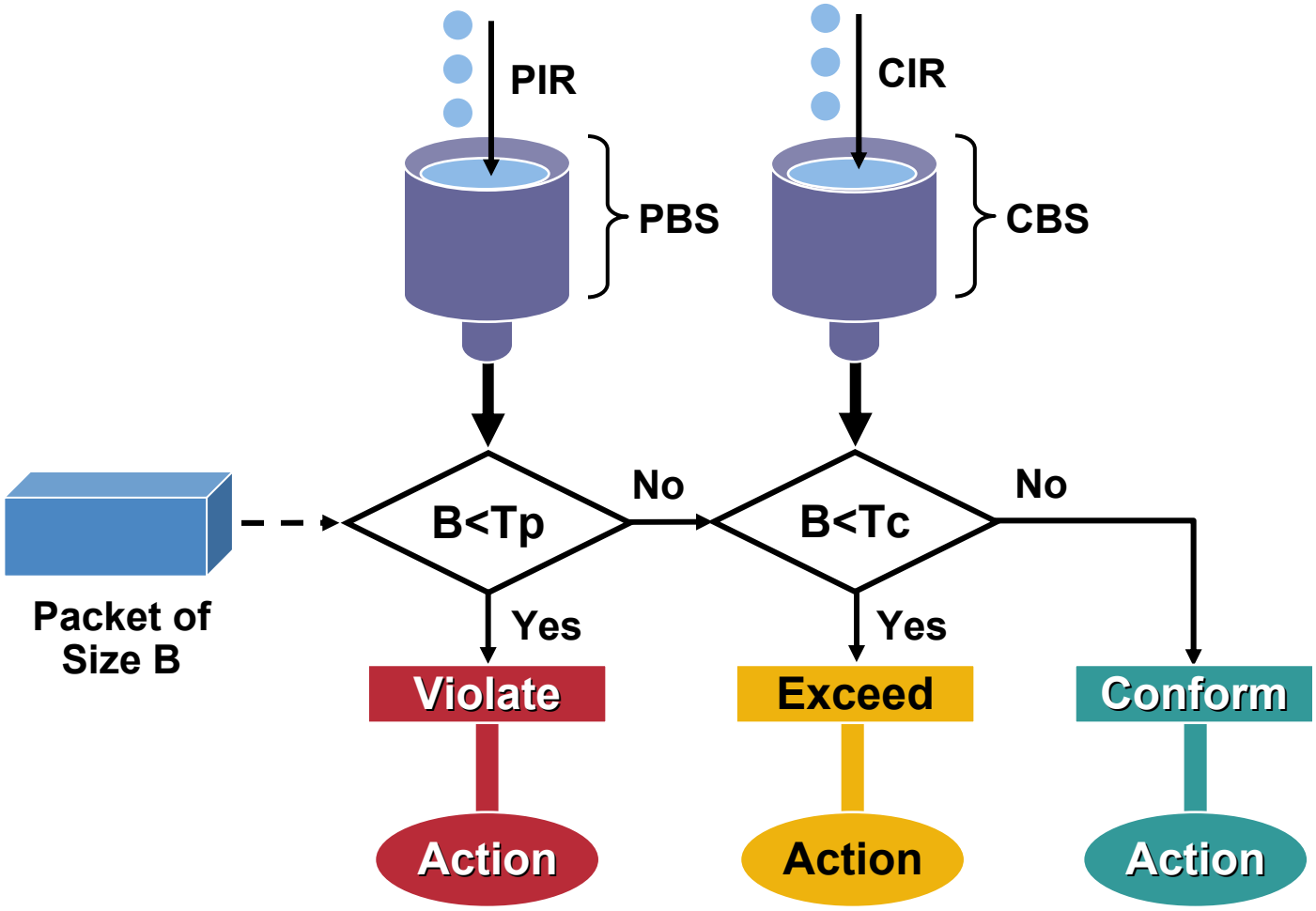
Policing Tools

RFC 2697 Single Rate Three Color Policer



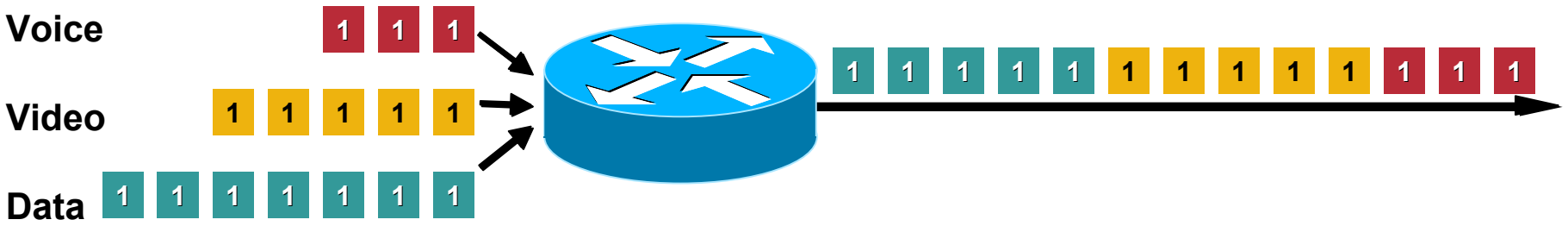
Policing Tools
RFC 2698 Two Rate Three Color Policer

Cisco.com



Scheduling Tools
Queuing Algorithms

Cisco.com

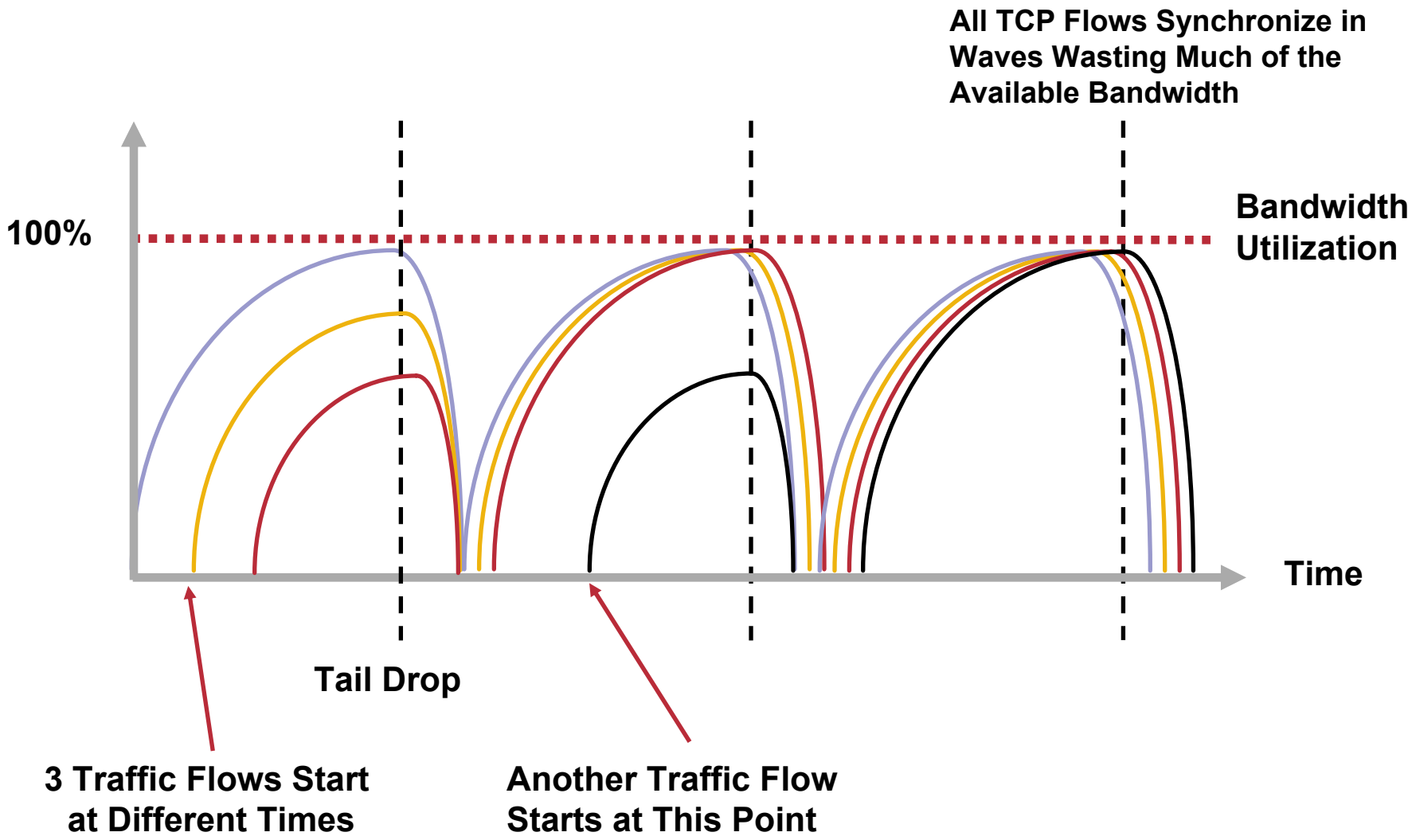


- Congestion can occur at any point in the network where there are speed mismatches
- Routers use Cisco IOS-based software queuing
  - Low-Latency Queuing (LLQ) used for highest-priority traffic (voice/video)
  - Class-Based Weighted-Fair Queuing (CBWFQ) used for guaranteeing bandwidth to data applications
- Cisco Catalyst® switches use hardware queuing

Scheduling Tools

TCP Global Synchronization: The Need for Congestion Avoidance

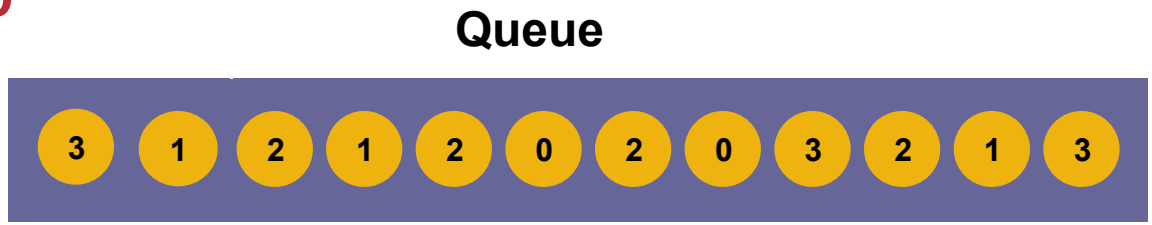
Cisco.com



Scheduling Tools
Congestion Avoidance Algorithms

Cisco.com

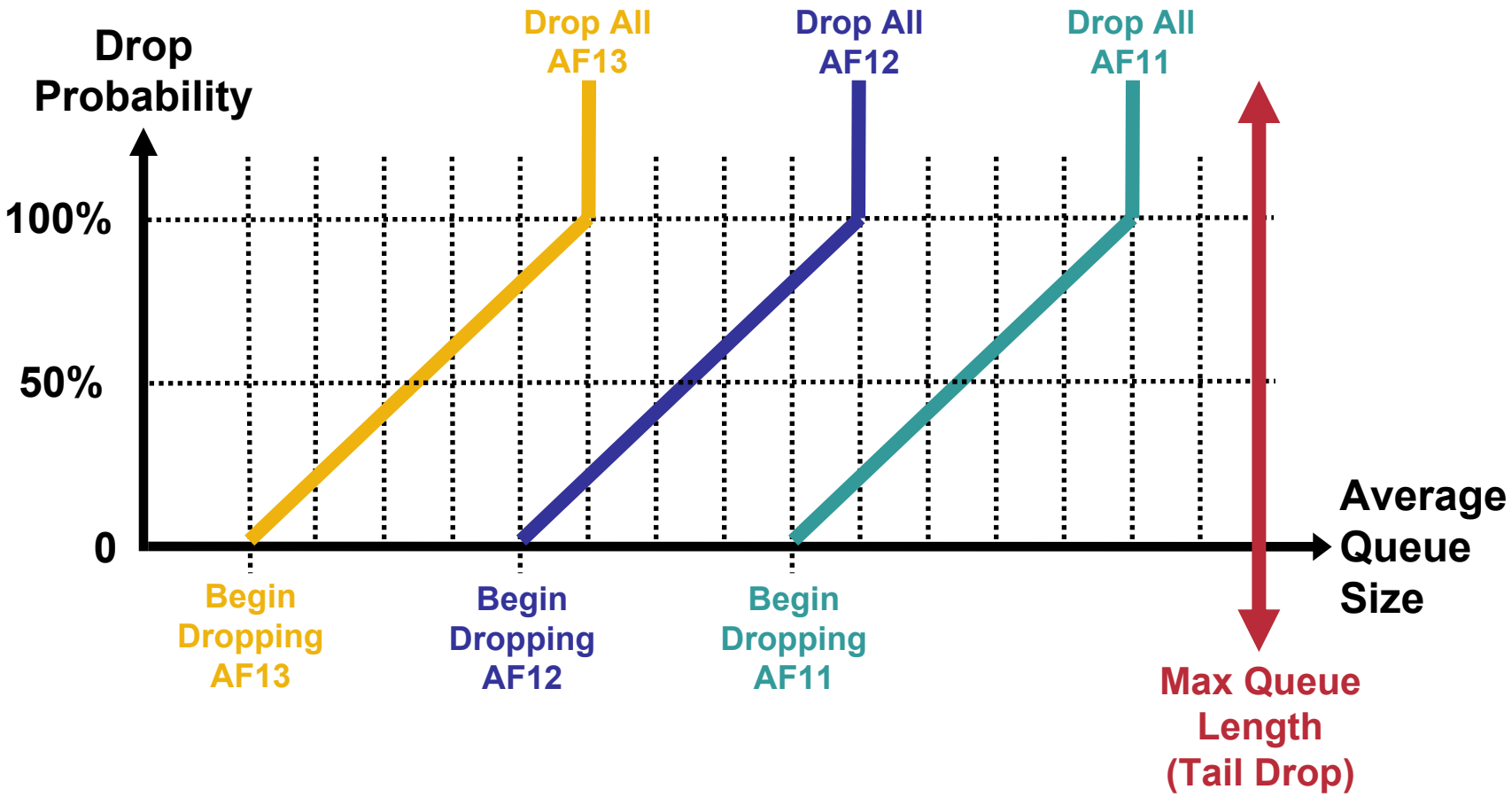
WRED



- Queueing algorithms manage the front of the queue
  - i.e. which packets get transmitted first
- Congestion avoidance algorithms, like Weighted-Random Early-Detect (WRED), manage the tail of the queue
  - i.e. which packets get dropped first when queuing buffers fill
- WRED can operate in a DiffServ compliant mode which will drop packets according to their DSCP markings
- WRED works best with TCP-based applications, like data

Scheduling Tools
DSCP-Based WRED Operation

Cisco.com

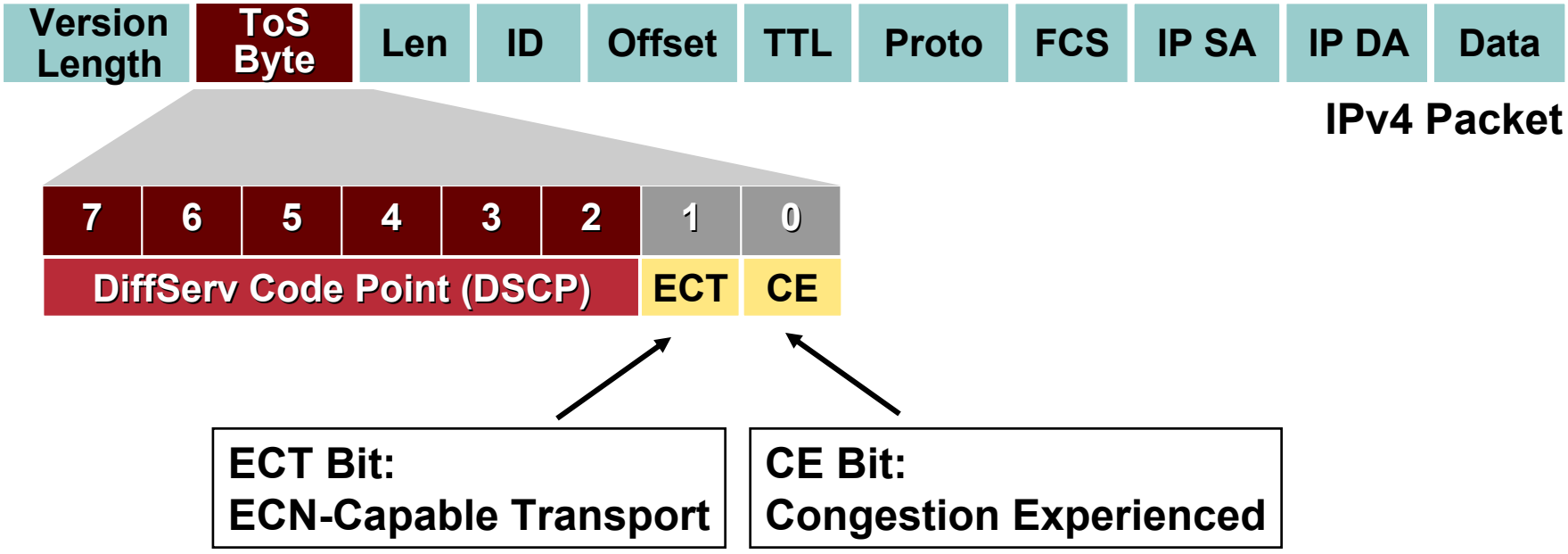


AF = (RFC 2597) Assured Forwarding

Congestion Avoidance Tools

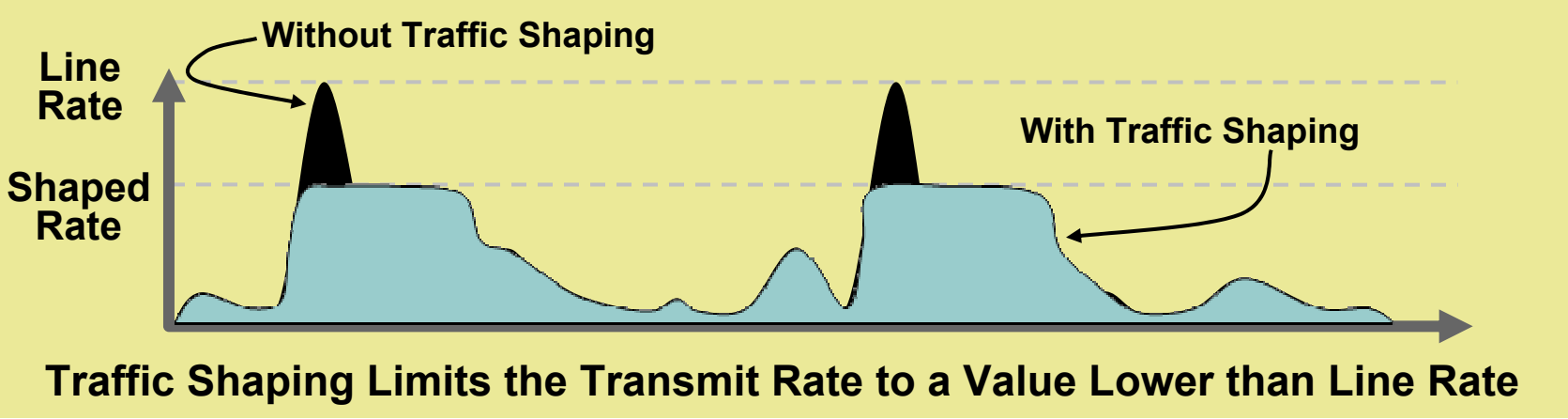
IP ToS Byte Explicit Congestion Notification (ECN) Bits

Cisco.com



RFC3168: IP Explicit Congestion Notification

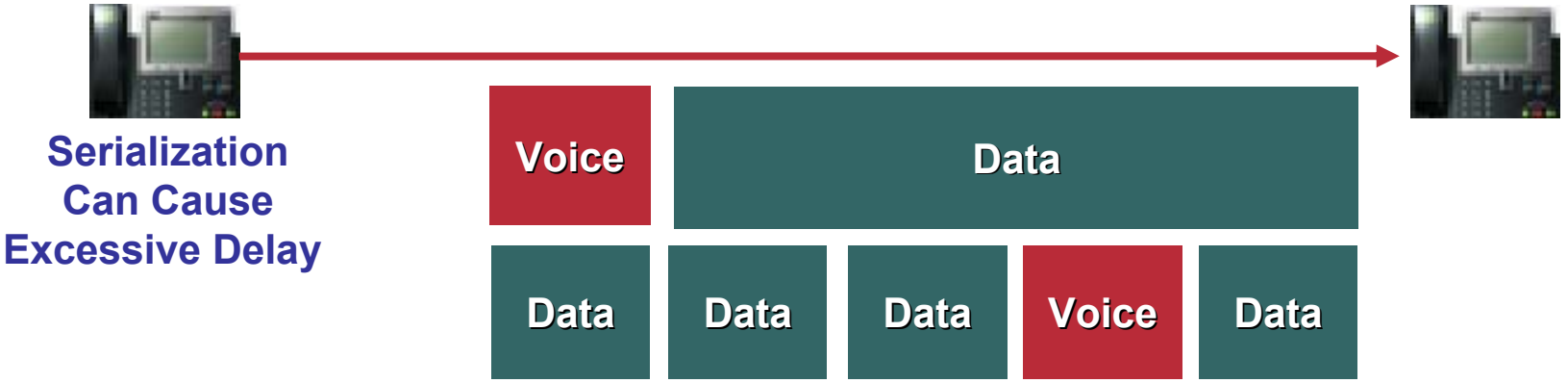
Shaping Tools
Traffic Shaping



- Policers typically drop traffic
- Shapers typically delay excess traffic, smoothing bursts and preventing unnecessary drops
- Very common on Non-Broadcast Multiple-Access (NBMA) network topologies such as Frame-Relay and ATM

Link-Specific Tools
Link-Fragmentation and Interleaving

Cisco.com

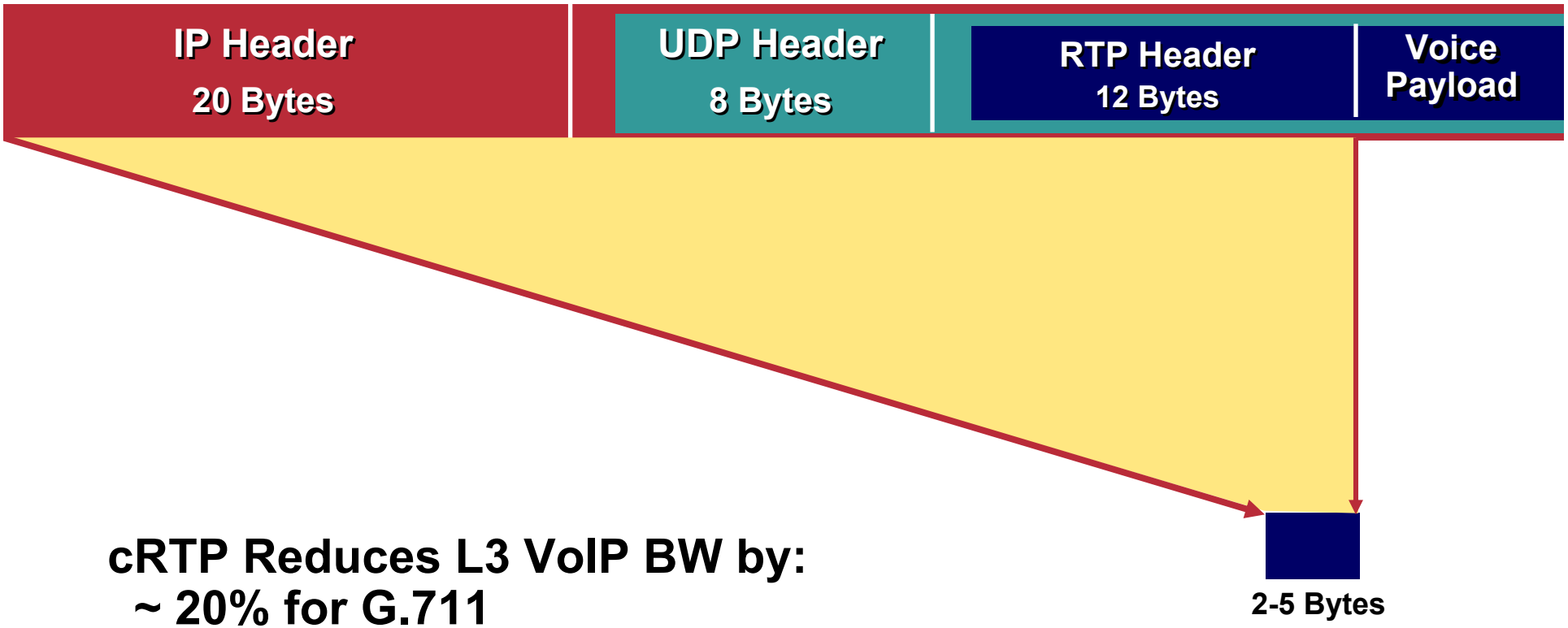


With Fragmentation and Interleaving Serialization Delay Is Minimized

- Serialization delay is the finite amount of time required to put frames on a wire
- For links ≤ 768 kbps serialization delay is a major factor affecting latency and jitter
- For such slow links, large data packets need to be fragmented and interleaved with smaller, more urgent voice packets

Link-Specific Tools
IP RTP Header Compression

Cisco.com



cRTP Reduces L3 VoIP BW by:
- **~ 20% for G.711**
- **~ 60% for G.729**

QOS DESIGN PRINCIPLES AND STRATEGIES

Voice QoS Requirements
Provisioning for Voice

Cisco.com

- Latency ≤ 150 ms
- Jitter ≤ 30 ms
- Loss ≤ 1%

One-Way Requirements

- 17–106 kbps guaranteed priority bandwidth per call
- 150 bps (+ Layer 2 overhead) guaranteed bandwidth for Voice-Control traffic per call
- CAC must be enabled

Voice

- Smooth
- Benign
- Drop sensitive
- Delay sensitive
- UDP priority

Video QoS Requirements
Provisioning for Interactive Video

Cisco.com

- Latency ≤ 150 ms
- Jitter ≤ 30 ms
- Loss ≤ 1%

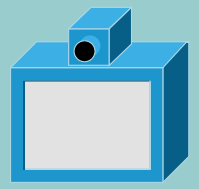
One-Way Requirements

- Minimum priority bandwidth guarantee required is:

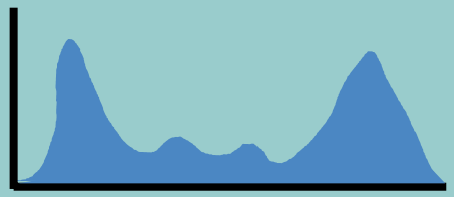
  Video-stream + 20%

  e.g. a 384 kbps stream would require 460 kbps of priority bandwidth

- CAC must be enabled



Video

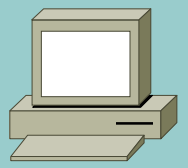


- Bursty
- Greedy
- Drop sensitive
- Delay sensitive
- UDP priority

Data QoS Requirements
Provisioning for Data

Cisco.com

- Different applications have different traffic characteristics
- Different versions of the same application can have different traffic characteristics
- Classify data into four/five data classes model:
  - Mission-critical apps
  - Transactional/interactive apps
  - Bulk data apps
  - Best effort apps
  - Optional: Scavenger apps



Data

- Smooth/bursty
- Benign/greedy
- Drop insensitive
- Delay insensitive
- TCP retransmits

Data QoS Requirements
Provisioning for Data (Cont.)

Cisco.com

- **Use four/five main traffic classes:**
  - **Mission-critical apps—business-critical client-server applications**
  - **Transactional/interactive apps—foreground apps: client-server apps or interactive applications**
  - **Bulk data apps—background apps: FTP, e-mail, backups, content distribution**
  - **Best effort apps—(default class)**
  - **Optional: Scavenger apps—peer-to-peer apps, gaming traffic**
- **Additional optional data classes include internetwork-control (routing) and network-management**
- **Most apps fall under best-effort, make sure that adequate bandwidth is provisioned for this default class**

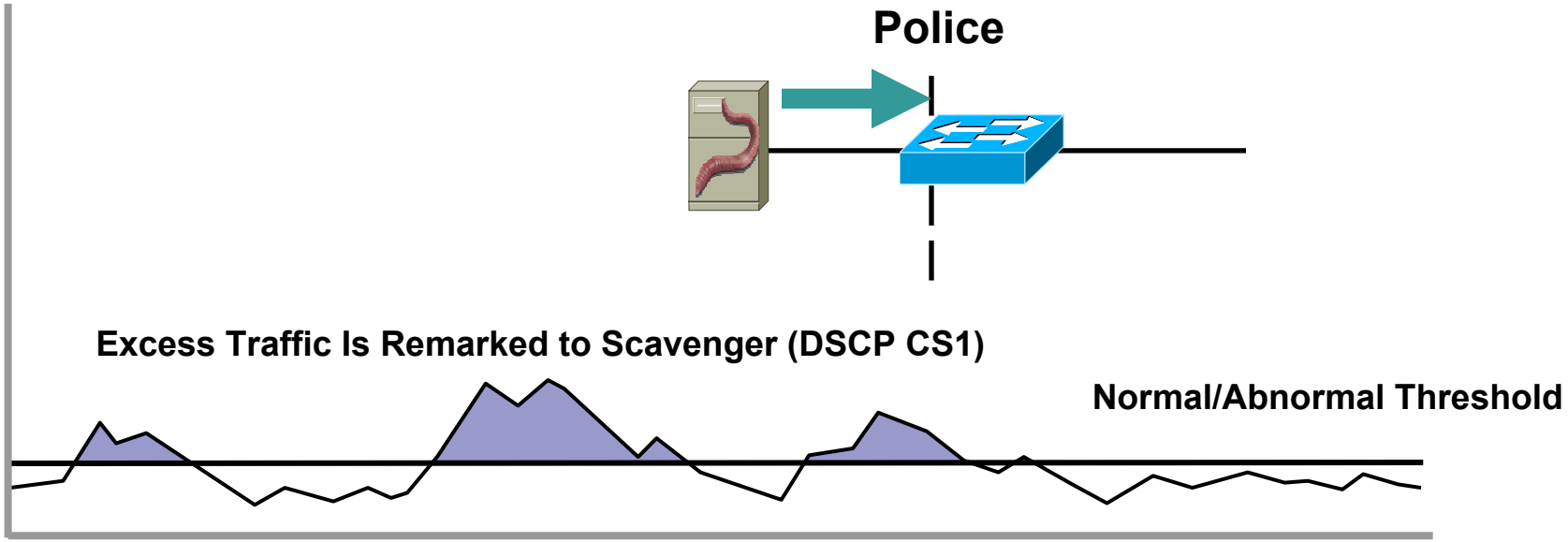
Scavenger-Class QoS DoS/Worm Mitigation Strategy
What Is the Scavenger Class?

Cisco.com

- The Scavenger class is an Internet 2 Draft Specification for a “less-than best effort” service
- There is an implied “good faith” commitment for the “best effort” traffic class
  - It is generally assumed that at least some network resources will be available for the default class
- Scavenger class markings can be used to distinguish out-of-profile/abnormal traffic flows from in-profile/normal flows
  - The Scavenger class marking is DSCP CS1 (8)
- Scavenger traffic is assigned a “less-than best effort” queuing treatment whenever congestion occurs

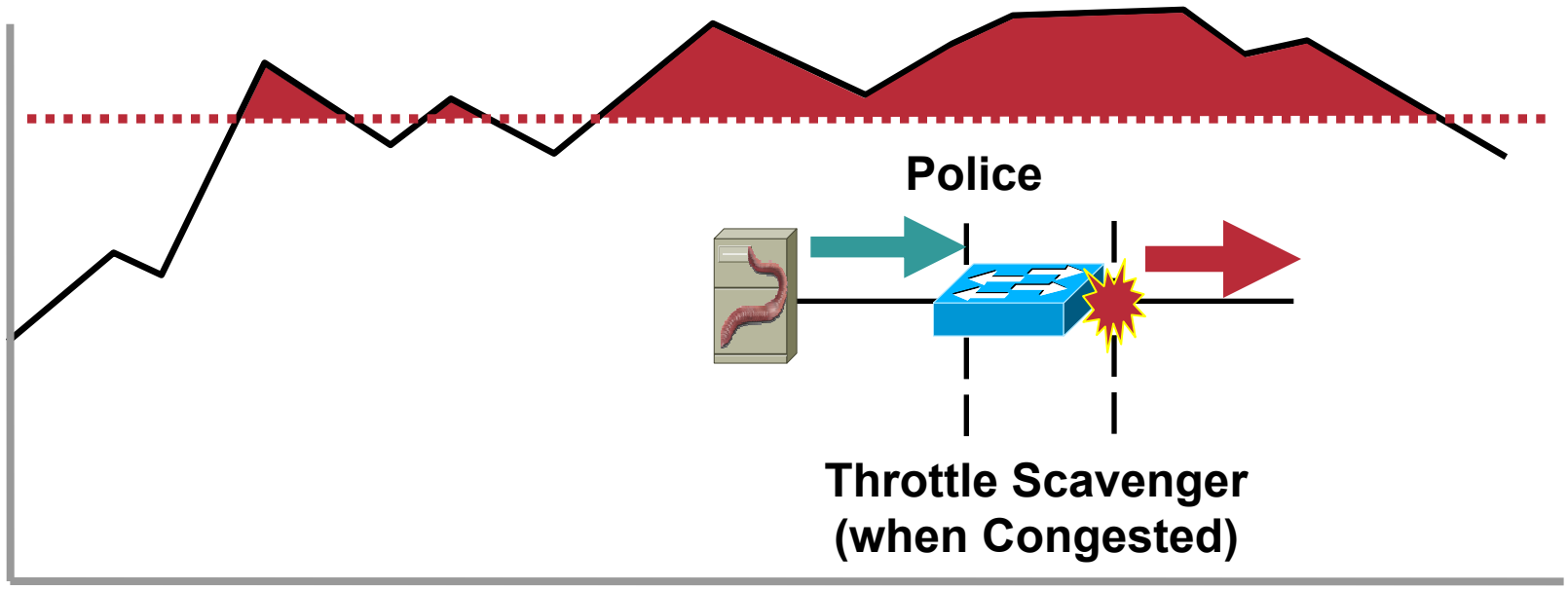
Scavenger-Class QoS DoS/Worm Mitigation Strategy
First Order Anomaly Detection

- All end systems generate traffic spikes
- Sustained traffic loads beyond ‘normal’ from each source device are considered suspect and marked as scavenger (DSCP CS1)
- No dropping at campus access-edge, only remarking



Scavenger-Class QoS DoS/Worm Mitigation Strategy
Second Order Anomaly Reaction

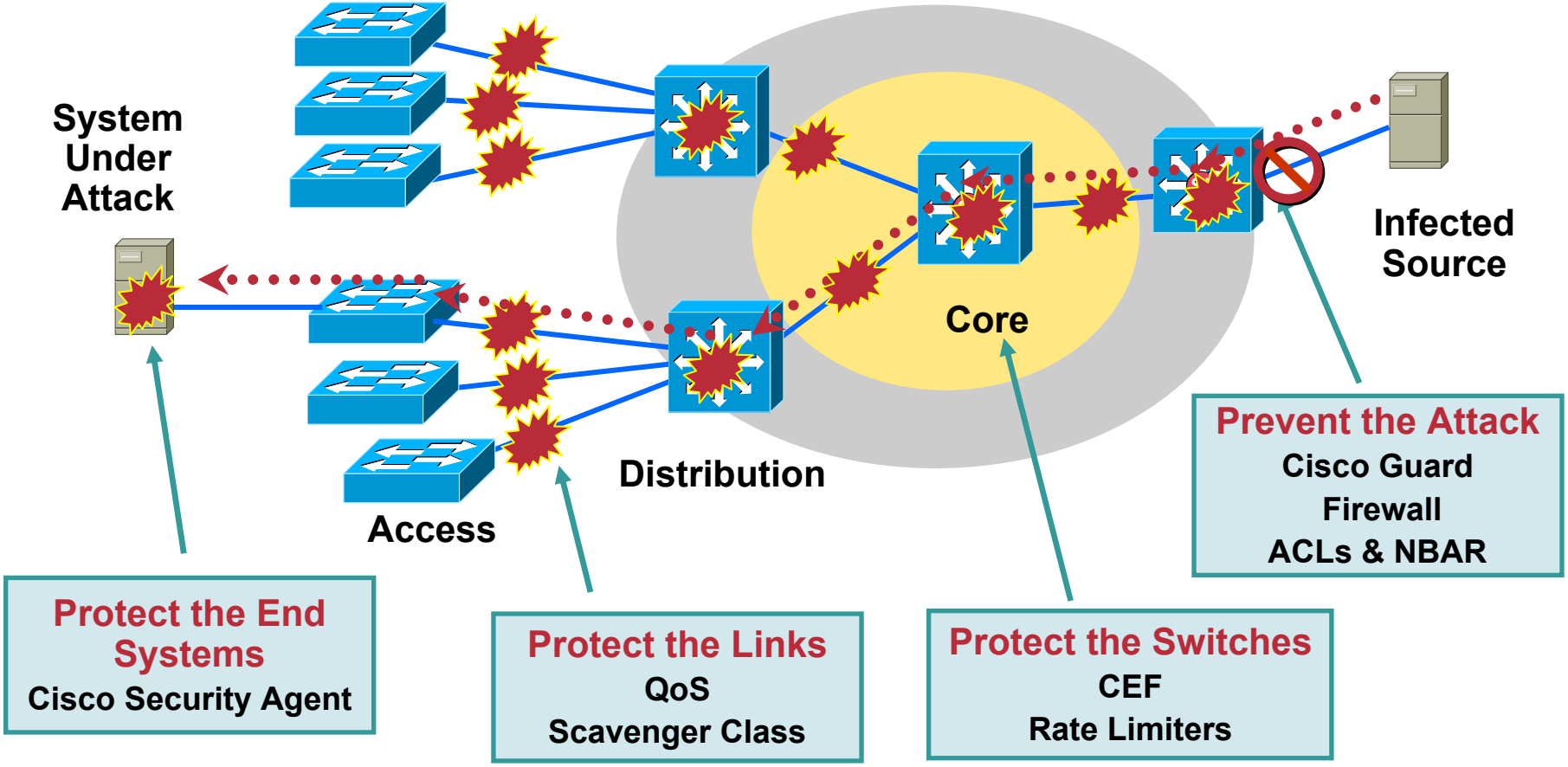
- During ‘abnormal’ worm traffic conditions traffic, where multiple infected hosts are causing uplink congestion, suspect traffic—previously marked as Scavenger—is aggressively dropped
- Stations not generating abnormal traffic volumes continue to receive network service



Scavenger-Class QoS DoS/Worm Mitigation Strategy

Preventing and Limiting the Pain

Cisco.com



An Integrated Network Architecture Holistically Combines High Availability, Quality of Service and Security Technologies to Prevent and Limit Attacks

Classification and Marking Design Principles
Where and How Should Marking Be Done?

Cisco.com

- QoS policies (in general) should always be performed in hardware, rather than software, whenever a choice exists
- Classify and mark applications as close to their sources as technically and administratively feasible
- Use DSCP markings whenever possible
- Follow standards-based DSCP PHBs to ensure interoperation and future expansion
  - RFC 2474 class selector code points
  - RFC 2597 assured forwarding classes
  - RFC 3246 expedited forwarding

Classification and Marking

QoS Baseline/AIT Marking Recommendations

Cisco.com

Application	L3 Classification			L2 CoS
	IPP	PHB	DSCP	
Routing	6	CS6	48	6
Voice	5	EF	46	5
Video Conferencing	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	-	25	3
Call Signaling	3	AF31 → CS3*	26 → 24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Scavenger	1	CS1	8	1
Best Effort	0	0	0	0

Policing Design Principles
Where and How Should Policing Be Done?

Cisco.com

- **Police traffic flows as close to their sources as possible**
- **Perform markdown according to standards-based rules, whenever supported**
  - **RFC 2597 specifies how assured forwarding traffic classes should be marked down (AF11 → AF12 → AF13) which should be done whenever DSCP-based WRED is supported on egress queues**
  - **Cisco Catalyst platforms currently do not support DSCP-based WRED, so Scavenger-class remarking is a viable alternative**
  - **Additionally, non-AF classes do not have a standards-based markdown scheme, so Scavenger-class remarking is a viable option**

DoS/Worm Mitigation Design Principles
How Can QoS Tools Contain Attacks?

Cisco.com

- Profile applications to determine what constitutes “normal” vs. “abnormal” flows (within a 95% confidence interval)
- Deploy campus access-edge policers to remark abnormal traffic to Scavenger
  - DSCP CS1 (8)
- Deploy a second-line of defense at the Distribution-Layer via per-user microflow policing
  - Cisco Catalyst 6500 Sup720 (PFC3) only
- Provision end-to-end “less-than-Best-Effort” Scavenger-class queuing policies
  - Campus + WAN + VPN
- Police-to-drop known worms/variants via NBAR on branch routers

Queuing Design Principles
Where and How Should Queuing Be Done?

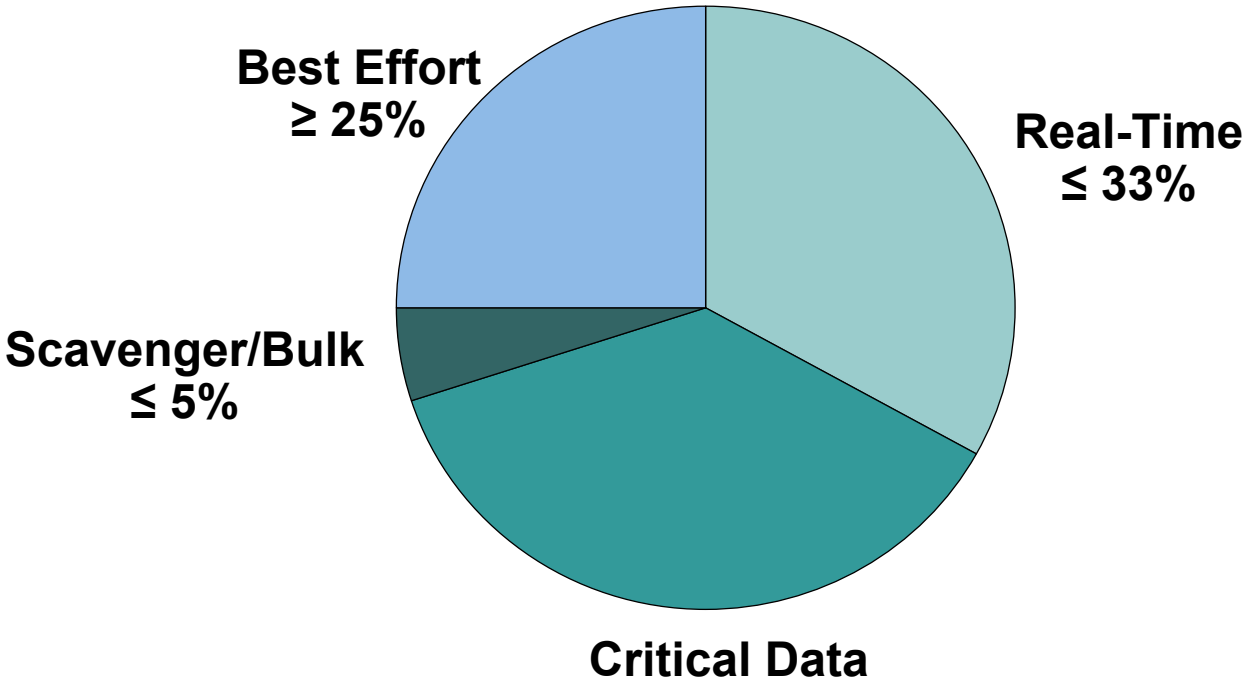
Cisco.com

- The only way to provide service GUARANTEES is to enable queuing at any node that has the potential for congestion
  - Regardless of how rarely—in fact—this may occur
- At least 25 percent of a link's bandwidth should be reserved for the default Best Effort class
- Limit the amount of strict-priority queuing to 33 percent of a link's capacity
- Whenever a Scavenger queuing class is enabled, it should be assigned a minimal amount of bandwidth
- To ensure consistent PHBs, configure consistent queuing policies in the Campus + WAN + VPN, according to platform capabilities
- Enable WRED on all TCP flows, whenever supported
  - Preferably DSCP-based WRED

Campus Queuing Design

Realtime, Best Effort and Scavenger Queuing Rules

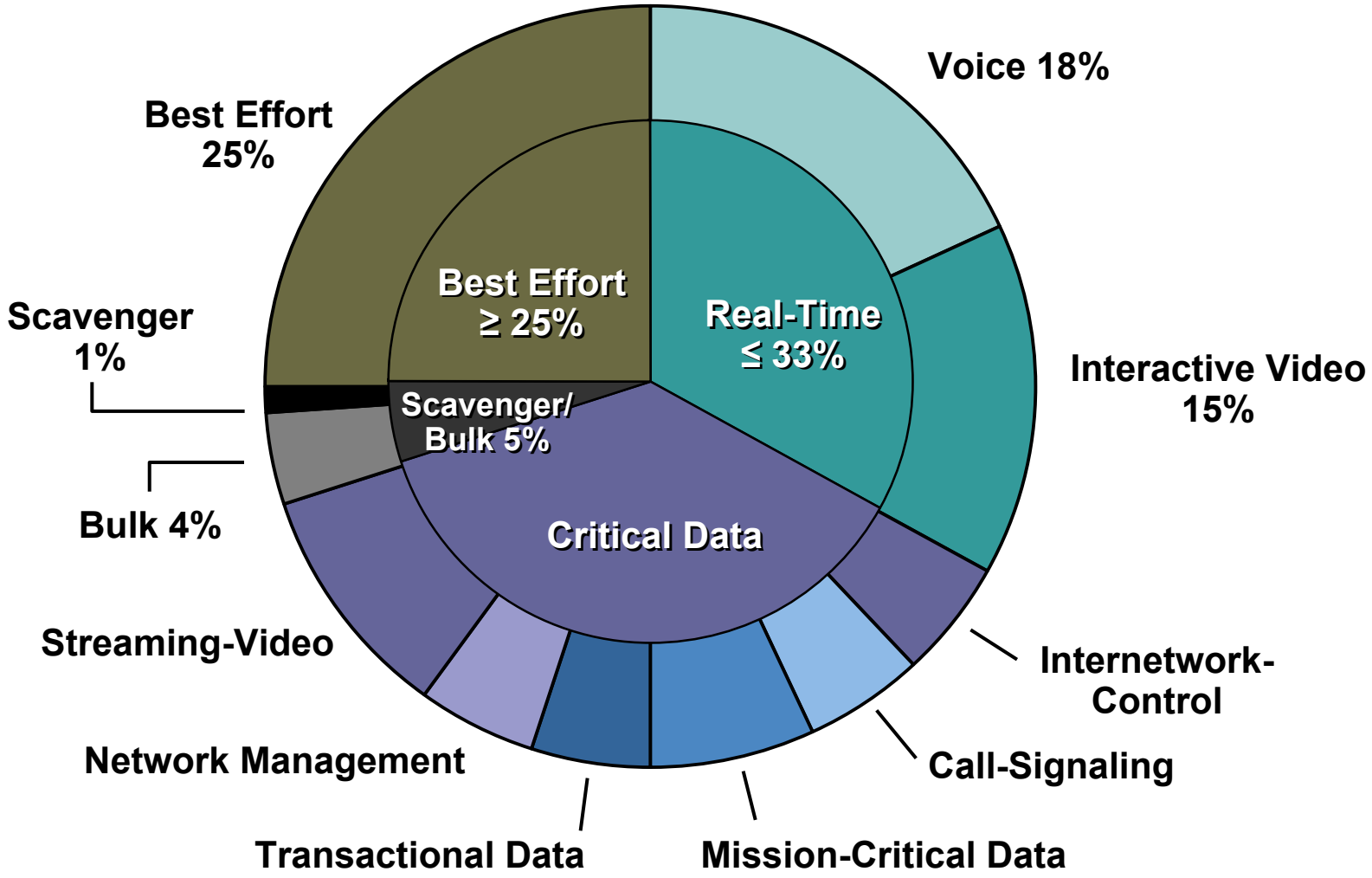
Cisco.com



Campus and WAN/VPN Queuing Design

Compatible Four-Class and Eleven-Class Queuing Models Following Realtime, Best Effort and Scavenger Queuing Rules

Cisco.com

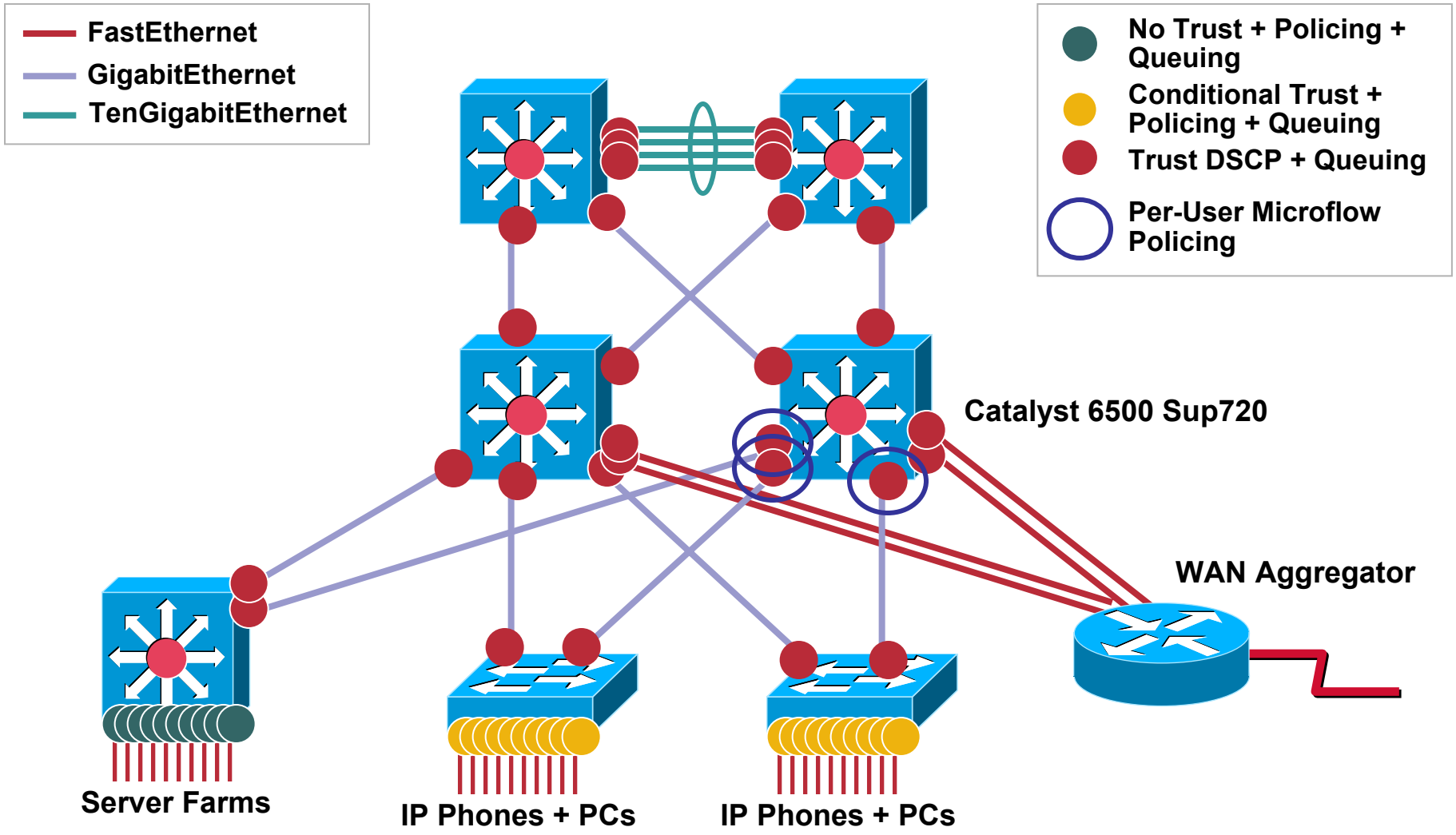


LAN/WAN/VPN QoS Design Overview

Campus QoS Considerations

Where Is QoS Required Within the Campus?

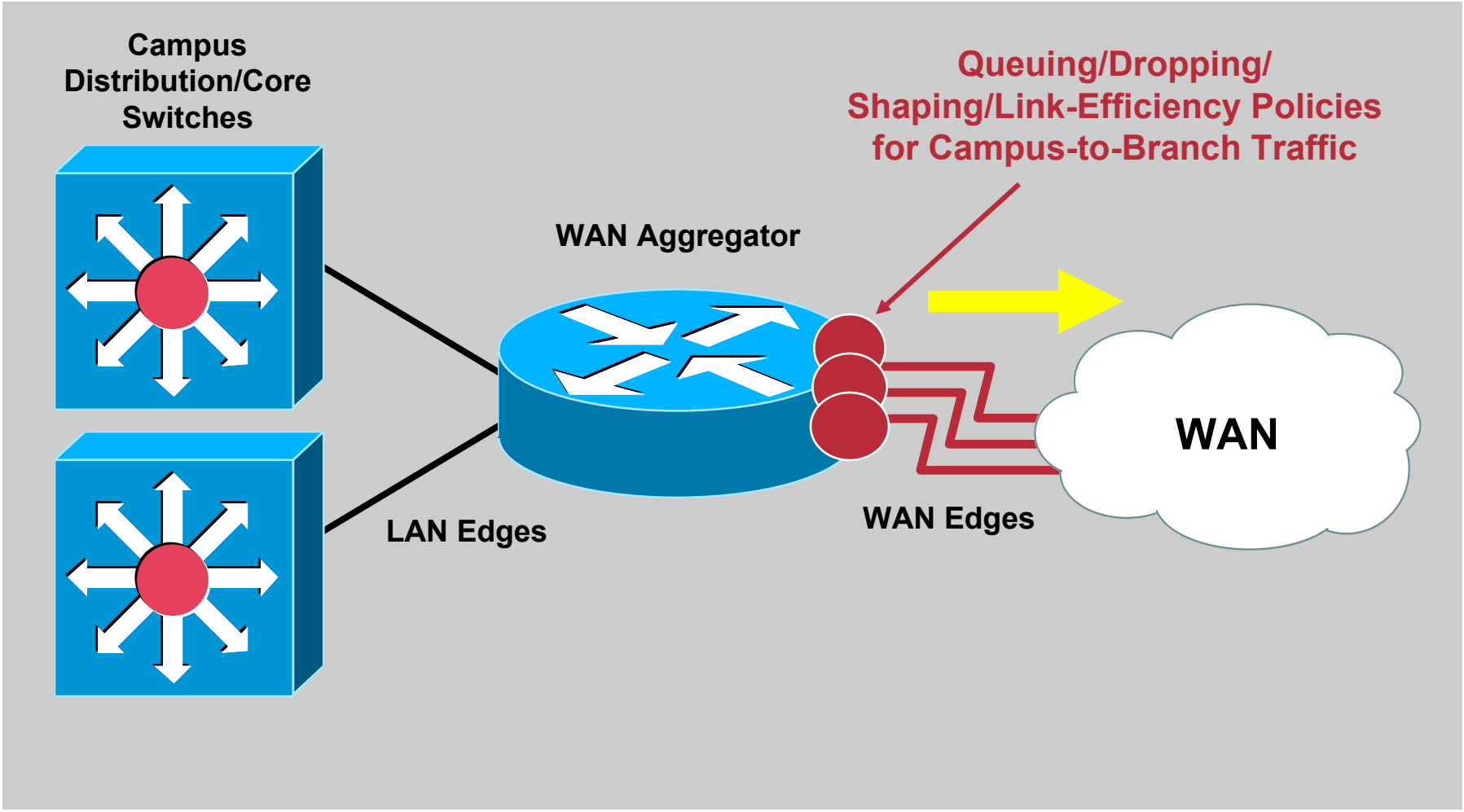
Cisco.com



WAN Edge QoS Design Considerations

QoS Requirements of WAN Aggregators

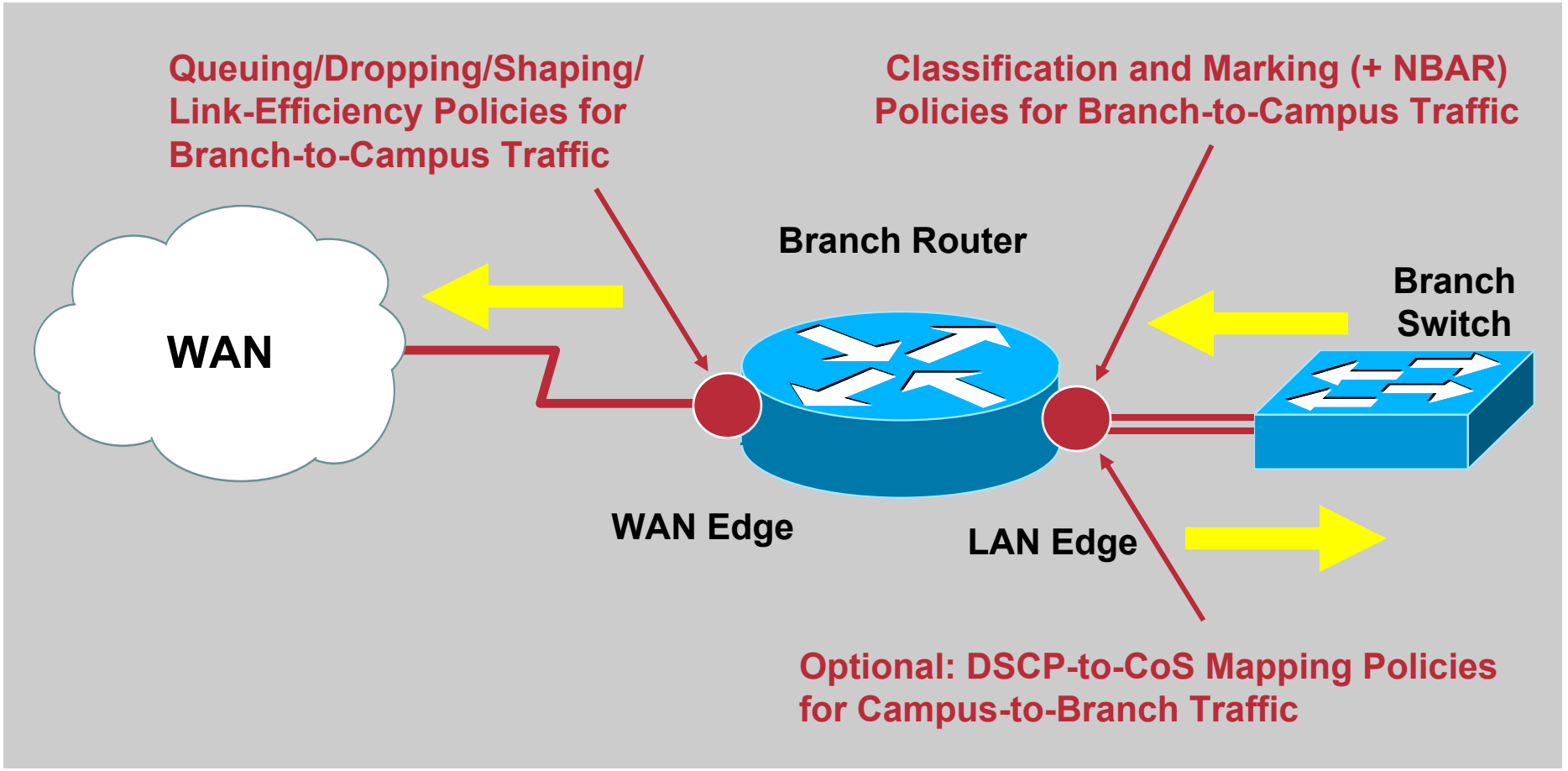
Cisco.com



Branch Router QoS Design

QoS Requirements for Branch Routers

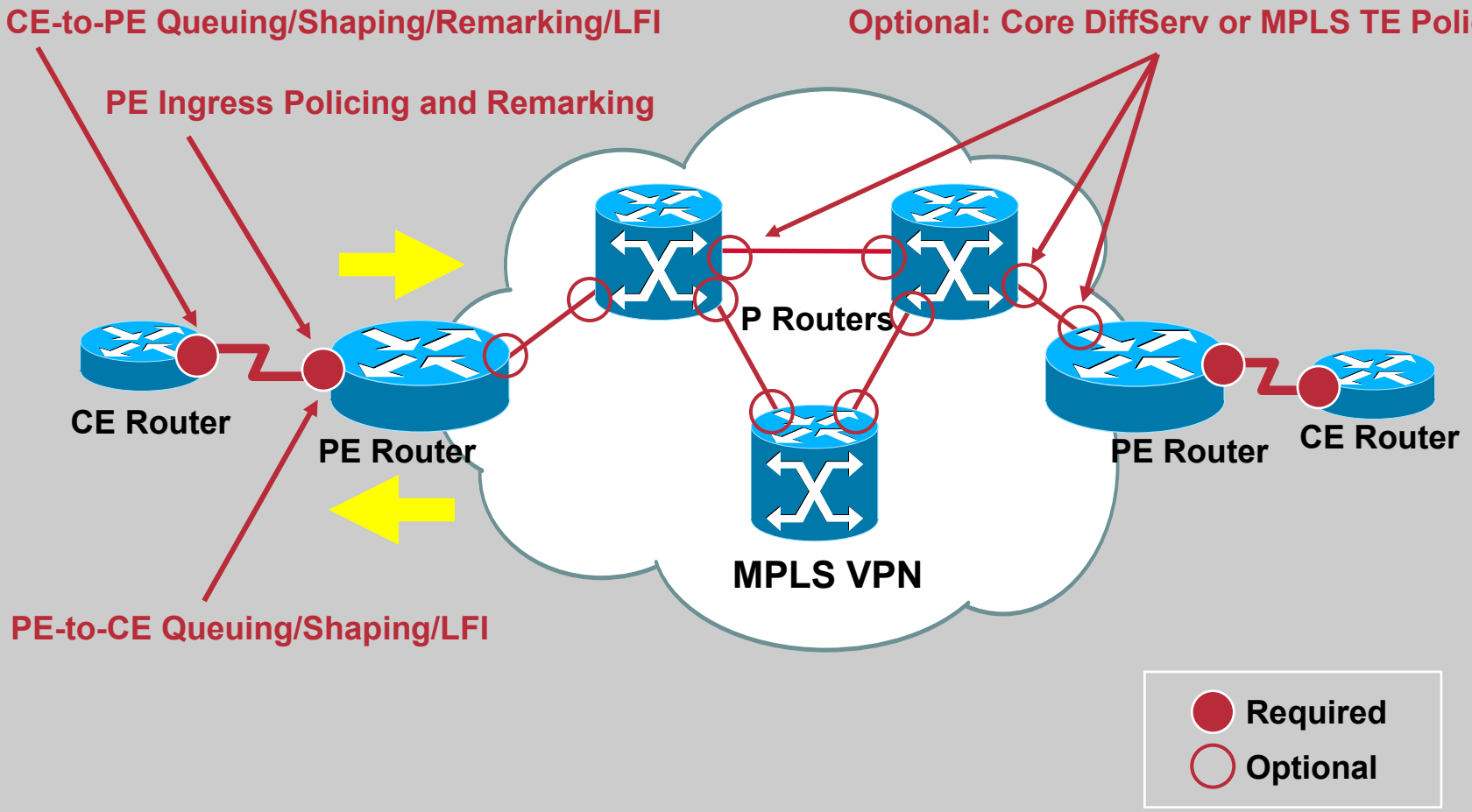
Cisco.com



MPLS VPN QoS Design

Where QoS Is Required in MPLS VPN Architectures?

Cisco.com



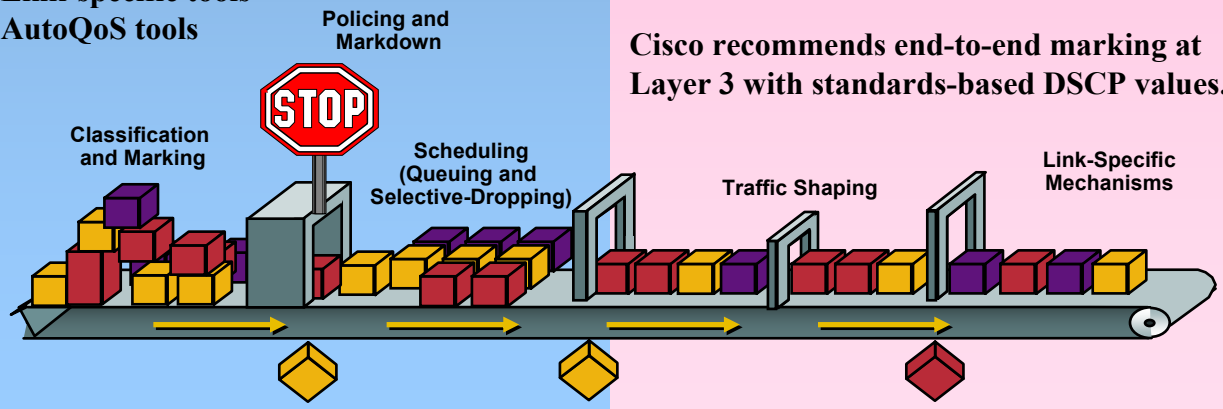
At-a-Glance Summaries

QoS Tools

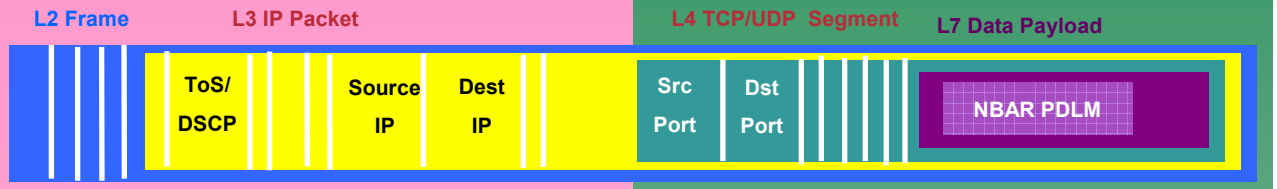
QoS is the measure of transmission quality and service availability of a network (or internetworks). The transmission quality of the network is determined by the following factors: Latency, Jitter and Loss.

QoS technologies refer to the set of tools and techniques to manage network resources and are considered the key enabling technologies for the transparent convergence of voice, video and data networks. Additionally, QoS tools can play a strategic role in significantly mitigating DoS/worm attacks.

Cisco's QoS toolset consists of the following:
- Classification and Marking tools
- Policing and Markdown tools
- Scheduling tools
- Link-specific tools
- AutoQoS tools

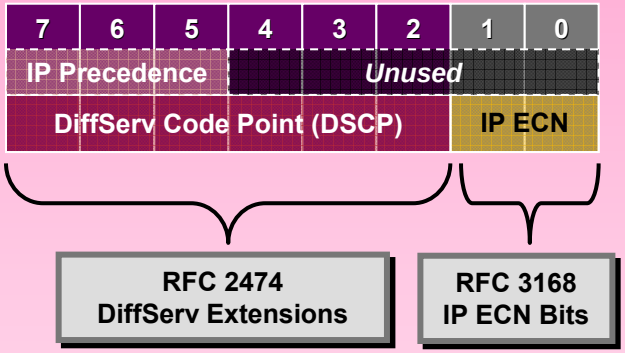


Classification can be done at Layers 2-7:



Marking can be done at Layers 2 or Layer 3:
Layer 2: 802.1Q/p CoS, MPLS EXP
Layer 3: IP Precedence, DSCP and/or IP ECN

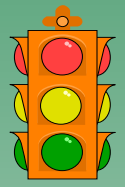
Layer 3 (IP ToS Byte) Marking Options:



Cisco recommends end-to-end marking at Layer 3 with standards-based DSCP values.

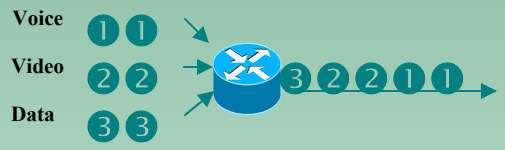
Policing tools can complement marking tools by marking metering flows and marking-down out-of-contract traffic.

Policers meter traffic into three categories:



- Conform: traffic is within the defined rate (green light)
- Exceed: moderate bursting is allowed (yellow light)
- Violate: no more traffic is allowed beyond this upper-limit (red light)

Scheduling tools re-order and selectively-drop packets whenever congestion occurs.



Link-Specific tools are useful on slow-speed WAN/VPN links and include shaping, compression, fragmentation and interleaving.

AutoQoS features automatically configure Cisco-recommend QoS on Catalyst switches and IOS routers with just one or two commands.

szigeti@cisco.com 2004

The QoS Baseline

The QoS Baseline is a strategic document designed to unify QoS within Cisco. The QoS Baseline provides uniform, standards-based recommendations to help ensure that QoS products, designs and deployments are unified and consistent.

The QoS Baseline defines up to 11 classes of traffic that may be viewed as critical to a given enterprise. A summary these classes and their respective standards-based markings and recommended QoS configurations are shown below.

Standards-based marking recommendations allow for better integration with service-provider offerings as well as other internetworking scenarios.

In Cisco IOS, rate-based queuing translates to CBWFQ; priority queuing is LLQ. DSCP-Based WRED (based on RFC 2597) drops AF*x*3 before AF*x*2, and in turn drops AF*x*2 before AF*x*1. RSVP is recommended (whenever supported) for Voice and/or Interactive-Video admission control

The IP Routing class is intended for IP Routing protocols, such as BGP, OSPF, etc.

The Call-Signaling class is intended for voice and/or video signaling traffic, such as Skinny, SIP, H.323, etc.

The Network Management class is intended for network management protocols, such as SNMP, Syslog, DNS, etc.

Application	L3 Classification PHB	L3 Classification DSCP	Referencing Standard	Recommended Configuration
IP Routing	CS6	48	RFC 2474-4.2.2	Rate-Based Queuing + RED
Voice	EF	46	RFC 3246	RSVP Admission Control + Priority Queuing
Interactive-Video	AF41	34	RFC 2597	RSVP + Rate-Based Queuing + DSCP-WRED
Streaming Video	CS4	32	RFC 2474-4.2.2	RSVP + Rate-Based Queuing + RED
Mission-Critical	AF31	26	RFC 2597	Rate-Based Queuing + DSCP-WRED
Call-Signaling	CS3	24	RFC 2474-4.2.2	Rate-Based Queuing + RED
Transactional Data	AF21	18	RFC 2597	Rate-Based Queuing + DSCP-WRED
Network Mgmt	CS2	16	RFC 2474-4.2.2	Rate-Based Queuing + RED
Bulk Data	AF11	10	RFC 2597	Rate-Based Queuing + DSCP-WRED
Scavenger	CS1	8	Internet 2	No BW Guarantee + RED
Best Effort	0	0	RFC 2474-4.1	BW Guarantee Rate-Based Queuing + RED

Interactive-Video refers to IP Video-Conferencing; Streaming Video is either unicast or multicast uni-directional video.

Cisco products that support QoS features will use these QoS Baseline recommendations for marking and scheduling and admission control.

The (Locally-Defined) Mission-Critical class is intended for a subset of Transactional Data applications that contribute most significantly to the business objectives (this is a non-technical assessment).

The Transactional Data class is intended for foreground, user-interactive applications such as database access, transaction services, interactive messaging and preferred data services.

The Bulk Data class is intended for background, non-interactive traffic flows, such as large file transfers, content distribution, database synchronization, backup operations and email.

The Scavenger class is based on an Internet 2 draft that defines a "less-than-Best Effort" service. In the event of link congestion, this class will be dropped the most aggressively.

The Best Effort class is also the default class. Unless an application has been assigned for preferential/deferential service, it will remain in this default class. Most enterprises have hundreds – if not thousands – of applications on their networks; the majority of which will remain in the Best Effort service class.

The QoS Baseline recommendations are intended as a standards-based guideline for customers – not as a mandate.

szigeti@cisco.com 2004

QoS Best-Practices

A successful QoS deployment includes three key phases:

1) Strategically defining the business objectives to be achieved via QoS.
2) Analyzing the service-level requirements of the traffic classes.
3) Designing and testing QoS policies

1) Strategically defining the business objectives to be achieved by QoS.

Business QoS objectives need to be defined:
- **Is the objective to enable VoIP only or is video also required?**
- **If so, is video-conferencing required or streaming video? Or both?**
- **Are there applications that are considered mission-critical? If so, what are they?**
- **Does the organization wish to squelch certain types of traffic? If so, what are they?**
- **Does the business want to use QoS tools to mitigate DoS/worm attacks?**
- **How many classes of service are needed to meet the business objectives?**

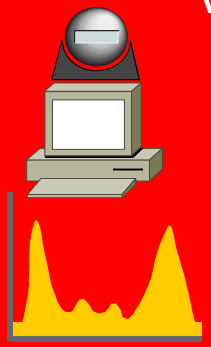
Because QoS introduces a system of managed unfairness, most QoS deployments inevitably entail political and organizational repercussions when implemented.

To minimize the effects of these non-technical obstacles to deployment, address these political and organizational issues as early as possible, garnishing executive endorsement whenever possible.

2) Analyze the application service-level requirements.

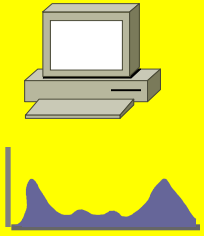
Voice

- Predicable Flows
- Drop + Delay Sensitive
- UDP Priority
- 150 ms one-way delay
- 30 ms jitter
- 1% loss
- 17 kbps-106 kbps VoIP + Call-Signaling



Video

- Unpredicable Flows
- Drop + Delay Sensitive
- UDP Priority
- 150 ms one-way delay
- 30 ms jitter
- 1% loss
- Overprovision stream by 20% to account for headers + bursts



Data

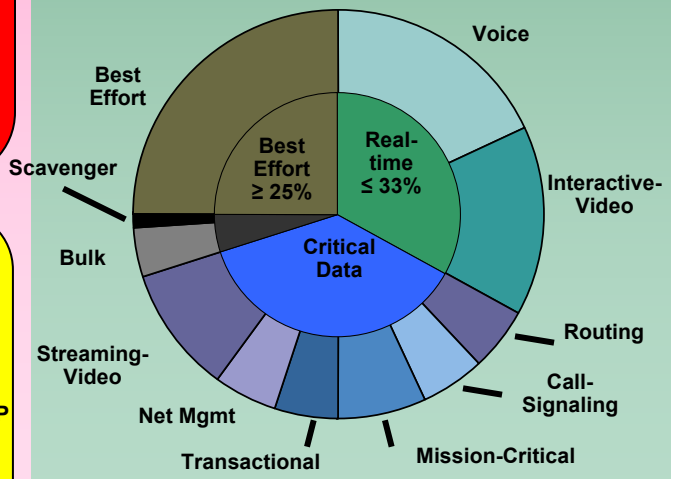
- No “one-size fits all”
- Smooth/Bursty
- Benign/Greedy
- TCP Retransmits/ UDP does not

3) Design and test the QoS Policies.

Classify, mark and police as close to the traffic-sources as possible; following Differentiated-Services standards, such as RFC 2474, 2475, 2597, 2698 and 3246.

Application	L3 Classification PHB	DSCP
Routing	CS6	48
Voice	EF	46
Interactive-Video	AF41	34
Streaming Video	CS4	32
Mission-Critical	AF31	26
Call-Signaling	CS3	24
Transactional Data	AF21	18
Network Mgmt	CS2	16
Bulk Data	AF11	10
Scavenger	CS1	8
Best Effort	0	0

Provision queuing in a consistent manner (according to platform capabilities).



Thoroughly test QoS policies prior to production-network deployment.

szigeti@cisco.com 2004

Scavenger-Class QoS Strategy for DoS/Worm Attack Mitigation

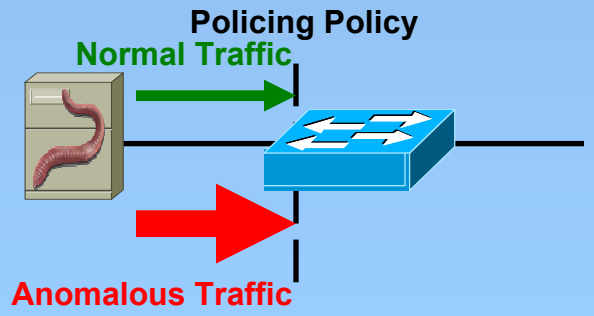
DoS and worm attacks are exponentially increasing in frequency, complexity and scope of damage. QoS tools and strategic designs can mitigate the effects of worms and keep critical applications available during DoS attacks.

One such strategy, referred to as Scavenger-class QoS, uses a two-step tactical approach to provide first- and second-order anomaly detection and reaction to DoS/worm attack-generated traffic.

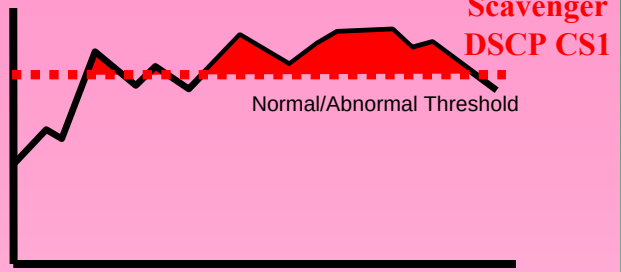
The first step in deploying Scavenger-class QoS is to profile applications to determine what constitutes a normal vs. abnormal flow (within a 95% confidence interval).

Application traffic exceeding this normal rate will be subject to first-order anomaly detection at the Campus Access-Edge, specifically: excess traffic will be marked down to Scavenger (DSCP CS1/8).

Note that anomalous traffic is not dropped or penalized at the edge; it is simply remarked.



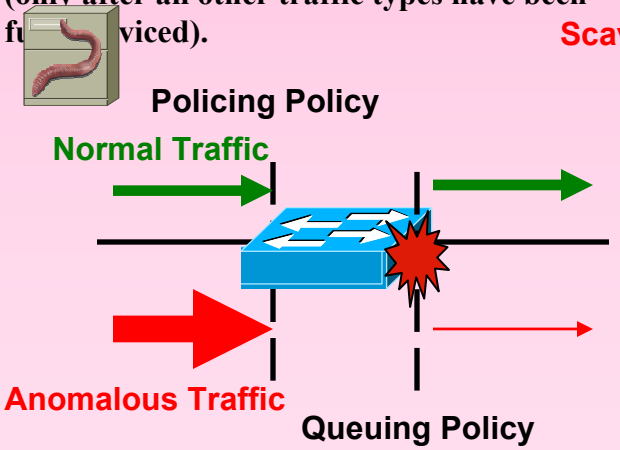
Only traffic in excess of the normal/abnormal threshold is remarked to Scavenger.



Campus Access-Edge policing policies are coupled with Scavenger-class queuing policies on the uplinks to the Campus Distribution Layer.

Queuing policies only engage when links are congested. Therefore, only if uplinks become congested does traffic begin to be dropped.

Anomalous traffic – previously marked to Scavenger – is dropped the most aggressively (only after all other traffic types have been fu viced).

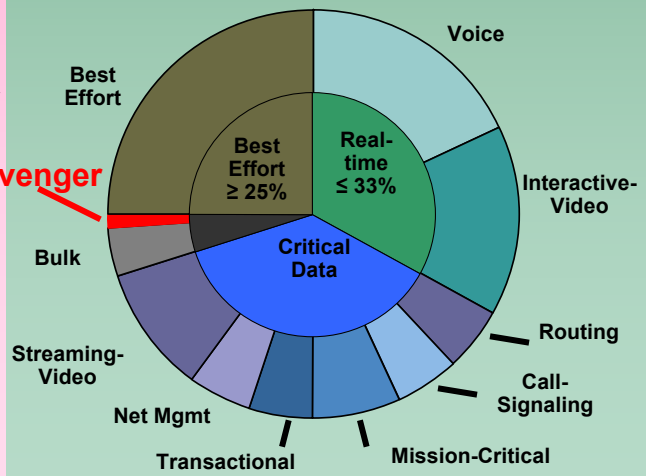


A key point of this strategy is that legitimate traffic flows that temporarily exceed thresholds are not penalized by Scavenger-class QoS.

Only sustained, abnormal streams generated simultaneously by multiple hosts (highly-indicative of DoS/worm attacks) are subject to aggressive dropping – and such dropping only occurs *after* legitimate traffic has been fully-serviced.

The Campus uplinks are not the only points in the network infrastructure that congestion could occur. Typically WAN and VPN links are the first to congest.

Therefore, Scavenger-class "less-than-Best-Effort" queuing should be provisioned on all network devices in a consistent manner (according to platform capabilities).



Thoroughly test QoS policies prior to production-network deployment.

szigeti@cisco.com 2004

Campus QoS Design

QoS policies should always be enabled in Catalyst switch hardware – rather than router software – whenever a choice exists.

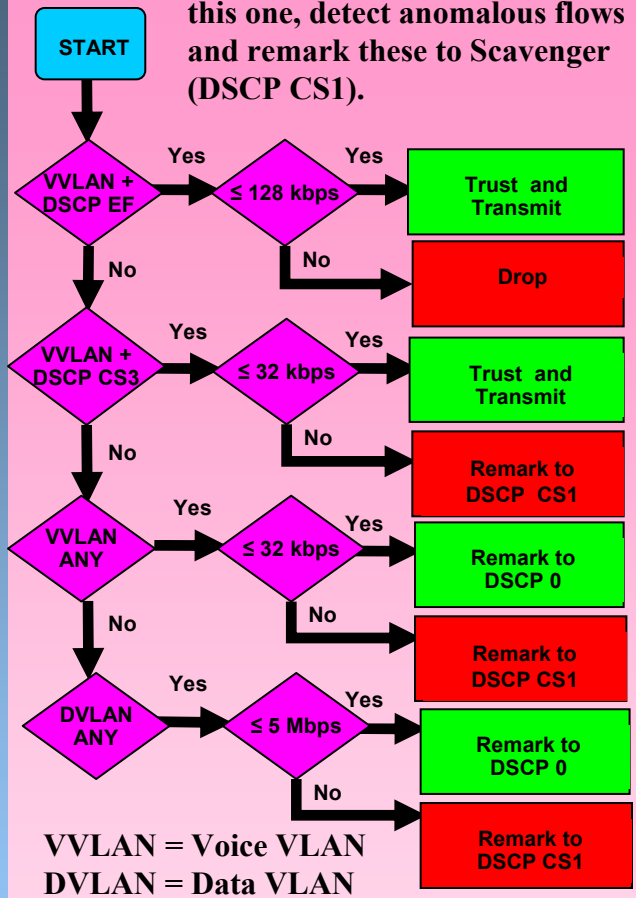
Three main types of QoS policies are required within the Campus:
1) Classification and Marking
2) Policing and Markdown
3) Queuing

Classification, marking and policing should be performed as close to the traffic-sources as possible, specifically at the Campus Access-Edge. Queuing, on the other hand, needs to be provisioned at all Campus Layers (Access, Distribution, Core) due to oversubscription ratios.

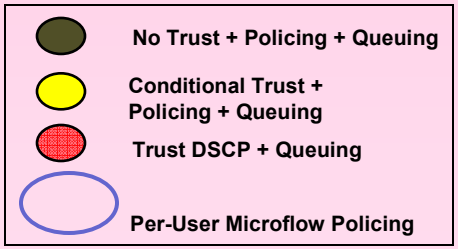
Classify and mark as close to the traffic-sources as possible following Cisco's QoS Baseline marking recommendations, which are based on Differentiated-Services standards, such as: RFC 2474, 2597 & 3246.

Application	L3 Classification PHB	DSCP
Routing	CS6	48
Voice	EF	46
Interactive-Video	AF41	34
Streaming Video	CS4	32
Mission-Critical	AF31	26
Call-Signaling	CS3	24
Transactional Data	AF21	18
Network Mgmt	CS2	16
Bulk Data	AF11	10
Scavenger	CS1	8
Best Effort	0	0

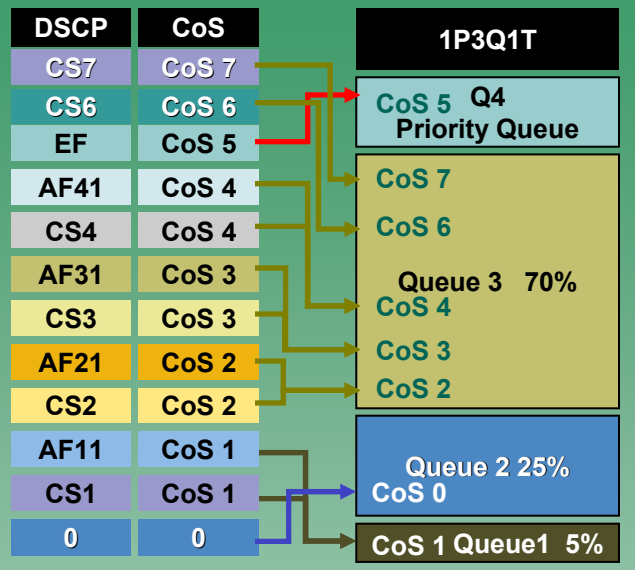
Access-Edge policers, such as this one, detect anomalous flows and remark these to Scavenger (DSCP CS1).



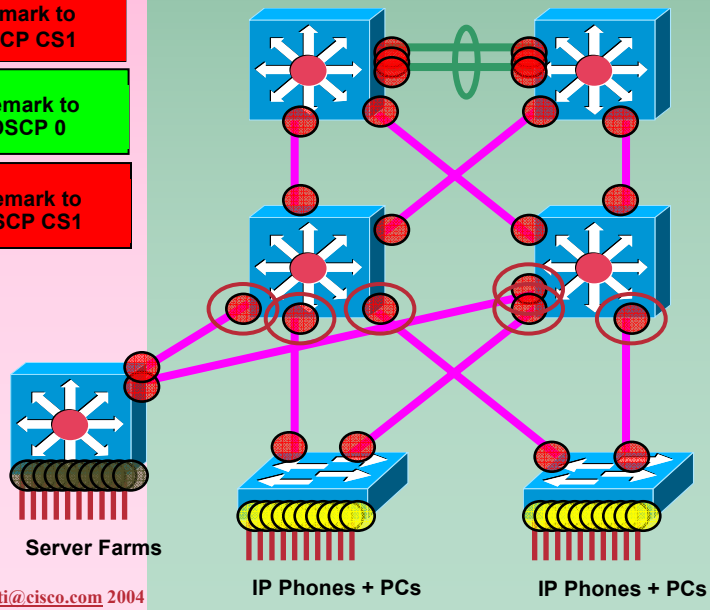
VVLAN = Voice VLAN
DVLAN = Data VLAN



Queuing policies will vary by platform:
E.g. 1P3Q1T P = Priority Queue
Q = Non-Priority Queue
T = WRED Threshold



The diagram below and left shows *what* QoS policies are needed *where* in the Campus.



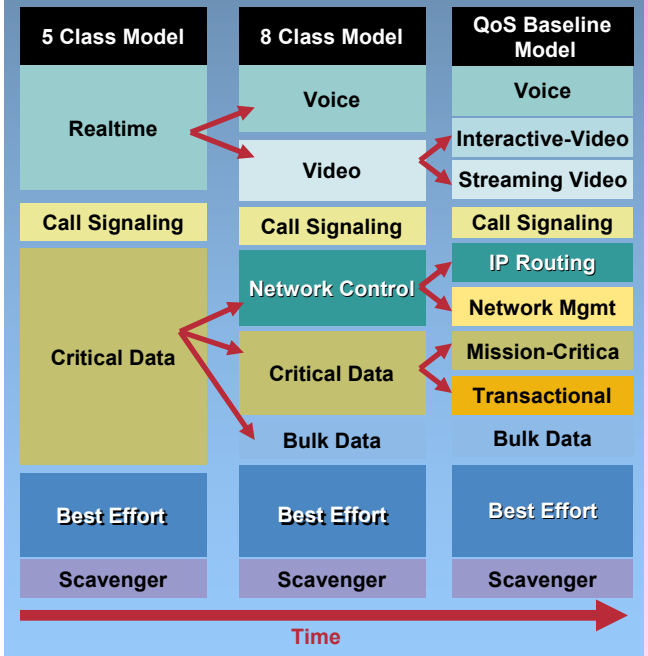
szigeti@cisco.com 2004

WAN QoS Design

In an enterprise network infrastructure, bandwidth is scarcest – and thus most expensive – over the WAN. Therefore, the business case for efficient bandwidth optimization via QoS technologies is strongest over the WAN.

WAN QoS policies need to be configured on the WAN edges of WAN Aggregator (WAG) routers and Branch routers. WAN edge QoS policies include queuing, shaping, selective-dropping and link-specific policies.

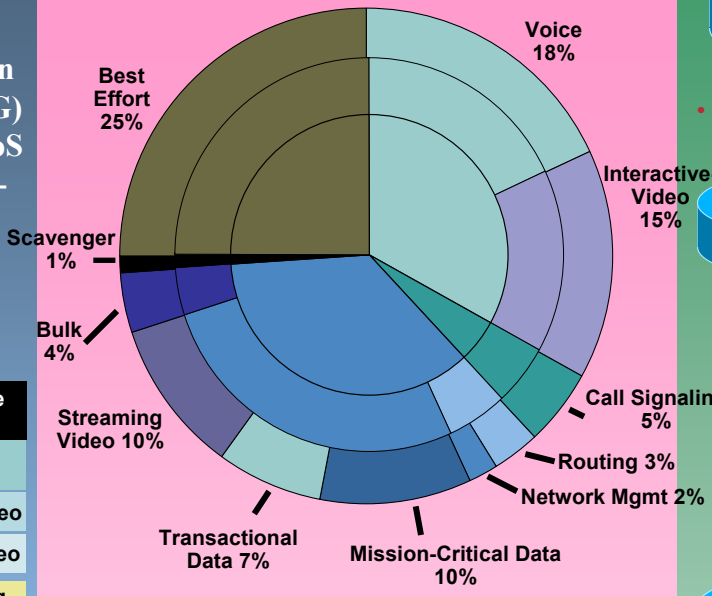
The number of WAN classes of traffic is determined by the business objectives and may be expanded over time.



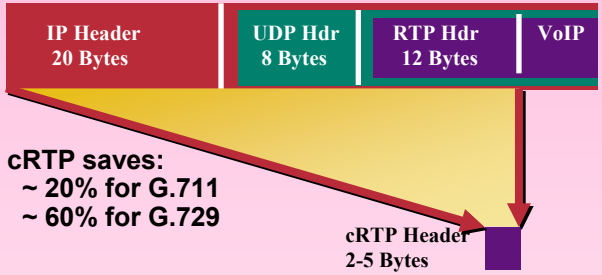
WAN links can be categorized into three main speed groups:

- Slow-Speed (≤ 768 kbps)
- Medium-Speed (> 768 kbps & ≤ T1/E1)
- High-Speed (≥ T1/E1)

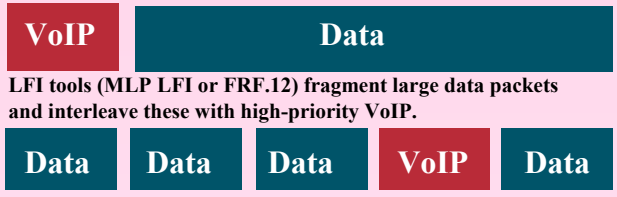
Queuing Models for 5/8/11 Classes of Service are shown below:



WAN QoS tools: RTP Header Compression (cRTP)



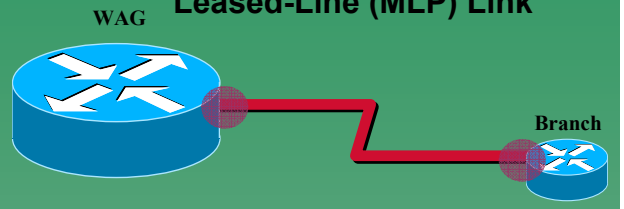
WAN QoS tools: Link Fragmentation and Interleaving



LFI tools (MLP LFI or FRF.12) fragment large data packets and interleave these with high-priority VoIP.

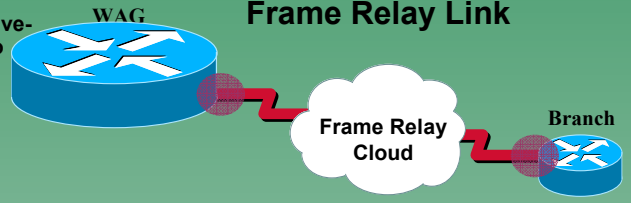
Link-Specific Design Recommendations:

Leased-Line (MLP) Link



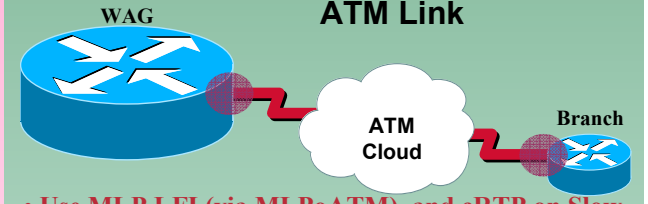
- Use MLP LFI and cRTP on Slow-Speed links

Frame Relay Link



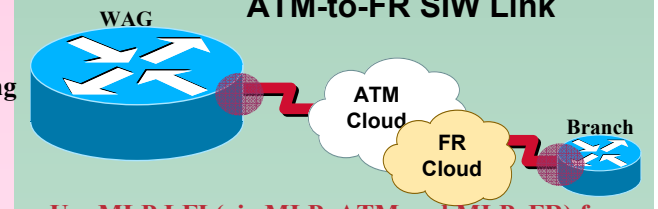
- Use Frame-Relay traffic shaping
  - Set CIR to 95% of guaranteed rate
  - Set Committed Burst to CIR/100
  - Set Excess Burst to 0
- Use FRF.12 and and cRTP on Slow-Speed links

ATM Link



- Use MLP LFI (via MLPoATM) and cRTP on Slow-Speed links
- Set the ATM PVC Tx-Ring to 3 for Slow-Speed links

ATM-to-FR SIW Link



- Use MLP LFI (via MLPoATM and MLPoFR) for Slow-Speed Links
- Optimize fragment sizes to minimize ATM cell-padding

szigeti@cisco.com 2004

Branch QoS Design

Branch routers are connected to central sites via private-WAN or VPN links which often prove to be the bottlenecks for traffic flows. QoS policies at these bottlenecks align expensive WAN/VPN bandwidth utilization with business objectives.

QoS designs for Branch routers are – for the most part – identical to WAN Aggregator QoS designs. However, Branch routers require three unique QoS considerations:

1) Unidirectional applications
2) Ingress classification requirements
3) NBAR policies for worm policing

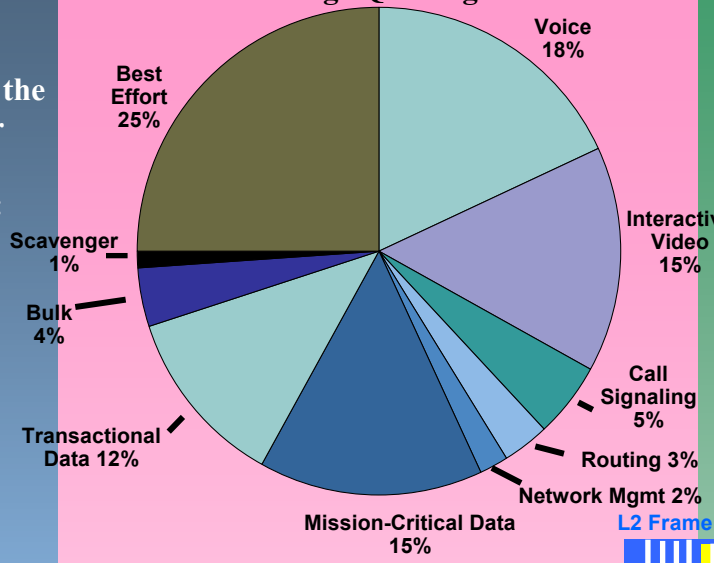
Each of these Branch router QoS design considerations will be overviewed.

1) Unidirectional Applications

Some applications (like Streaming Video) usually only traverse the WAN/VPN in the Campus-to-Branch direction and therefore do not require provisioning in the Branch-to-Campus direction on the Branch router's WAN edge.

Bandwidth for such unidirectional application classes can be reassigned to other critical classes, as shown in the following diagram. Notice that no Streaming Video class is provisioned and the bandwidth allocated to it (on the Campus side of the WAN link) is reallocated to the Mission-Critical and Transactional Data classes.

An example 10-class QoS Baseline Branch Router WAN Edge Queuing Model:



2) Ingress Classification

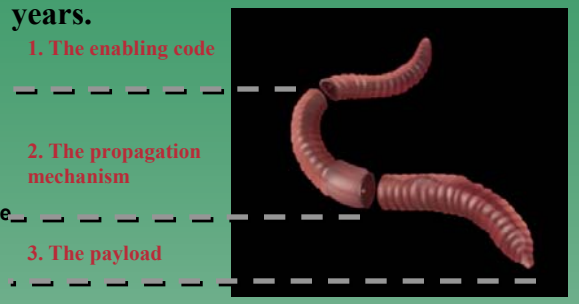
Branch-to-Campus traffic may not be correctly marked on the Branch Access Layer switch.

These switches – which are usually lower-end switches – may or may not have the capabilities to classify and mark application traffic. Therefore, classification and marking may need to be performed on the Branch router's LAN edge (in the ingress direction).

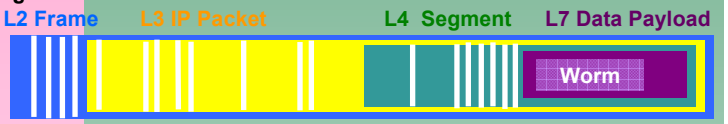
Furthermore, Branch routers offer the ability to use NBAR to classify and mark traffic flows that require stateful packet inspection.

3) NBAR for Known Worm Policing

Worms are nothing new, but they have increased exponentially in frequency, complexity and scope of damage in recent years.

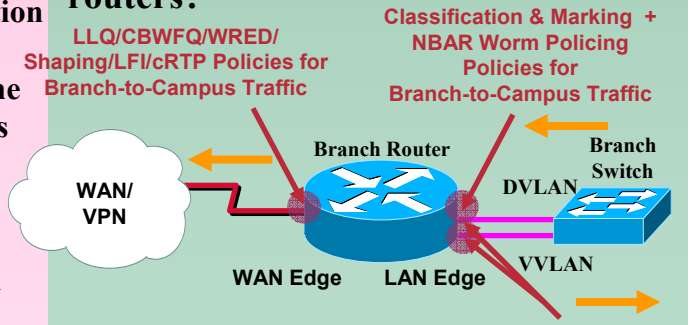


The Branch router's ingress LAN edge is a strategic place to use NBAR to identify & drop worms, such as CodeRed, NIMDA, SQL Slammer, MS-Blaster and Sasser.



NBAR extensions allow for custom Packet Data Language Modules (PDLMs) to be defined for future worms.

Where is QoS required on Branch routers?



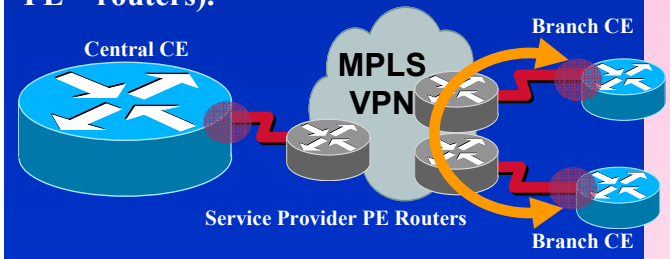
szigeti@cisco.com 2004

QoS Design for MPLS VPN Subscribers

QoS design for an enterprise subscribing to a MPLS VPN requires a major paradigm shift from private-WAN QoS design.

This is because with private-WAN design, the enterprise principally controlled QoS. The WAN Aggregator (WAG) provisioned QoS for not only Campus-to-Branch traffic, but also for Branch-to-Branch traffic (which was homed through the WAG).

However, due to the any-to-any/full-mesh nature of MPLS VPNs, Branch-to-Branch traffic is no longer homed through the WAG. While Branch-to-MPLS VPN QoS is controlled by the enterprise (on their Customer-Edge – CE – routers), MPLS VPN-to-Branch QoS is controlled by the service provider (on their Provider Edge – PE – routers).



Therefore, to guarantee end-to-end QoS, enterprises must co-manage QoS with their MPLS VPN service providers; their policies must be both consistent and complementary.

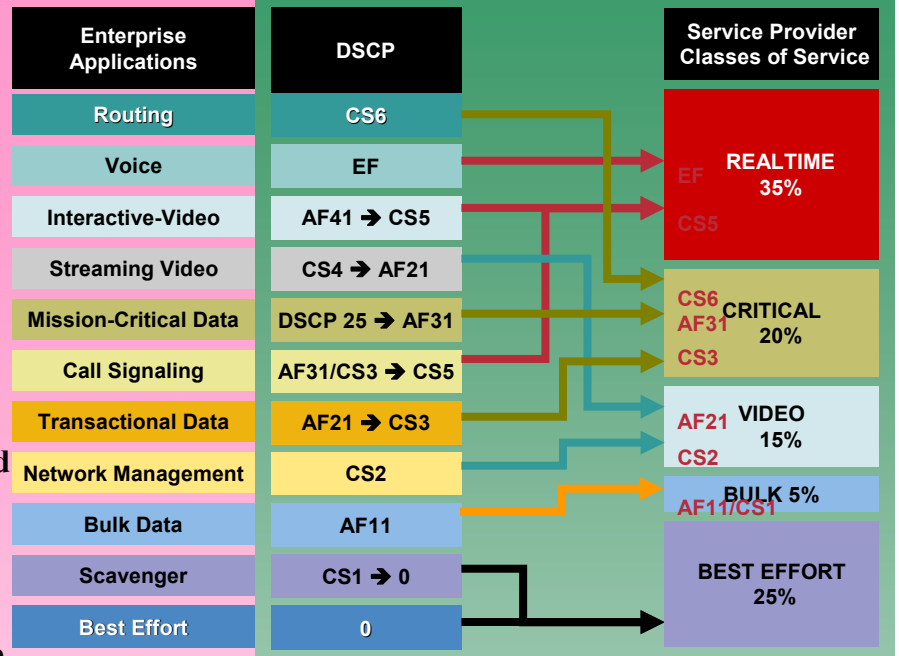
MPLS VPN service providers offer classes of service to enterprise subscribers.

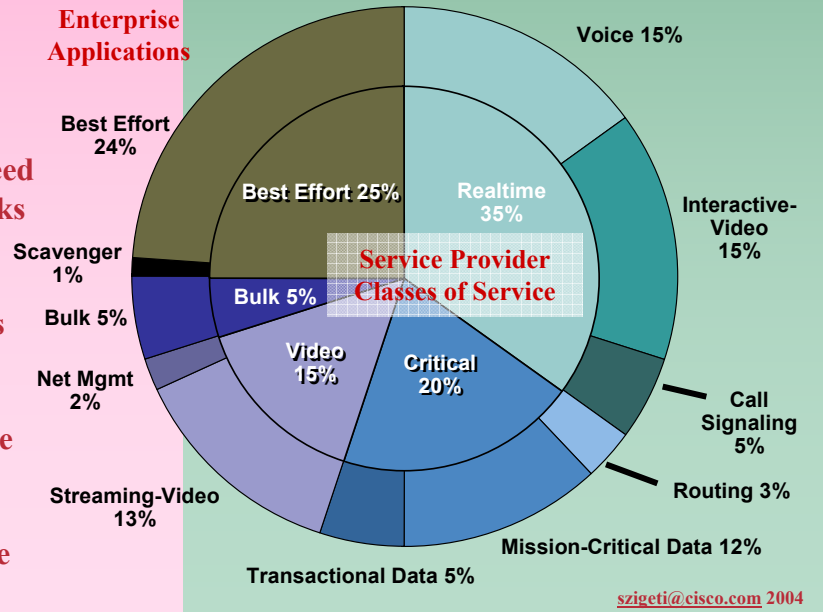
Admission criteria for these classes is the DSCP markings of enterprise traffic. Thus, enterprises may have to remark application traffic to gain admission into the required service provider class.

Some best practices to consider when assigning enterprise traffic to service provider classes of service include:

- Don't put Voice and Interactive-Video into the Realtime class on slow-speed (≤ 768 kbps) CE-to-PE links
- Don't put Call-Signaling into the Realtime class on slow-speed CE-to-PE links
- Don't mix TCP applications with UDP applications within a single service provider class (whenever possible); UDP applications may dominate the class when congested

Example enterprise subscriber DSCP Remarking Diagram and CE Edge Bandwidth Allocation Diagram.





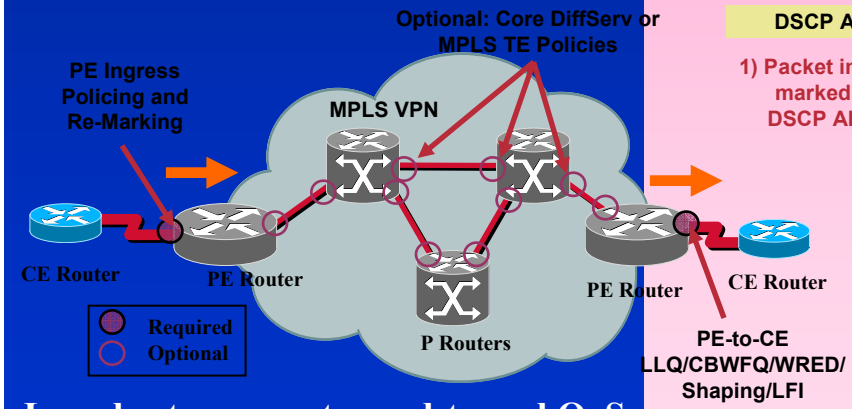
szigeti@cisco.com 2004

QoS Design for MPLS VPN Service Providers

In order to support enterprise-subscriber voice, video and data networks, service providers must include QoS provisioning within their MPLS VPN service offerings.

This is due to the any-to-any/full-mesh nature of MPLS VPNs, where enterprise subscribers depend on their service providers to provision Provider-Edge (PE) to Customer-Edge (CE) QoS policies consistent with their CE-to-PE policies.

In addition to these PE-to-CE policies, service providers will likely implement ingress policers on their PEs to identify whether traffic flows are in- or out-of-contract. Optionally, service providers may also provision QoS policies within their core networks, using Differentiated Services and/or MPLS Traffic Engineering (TE).

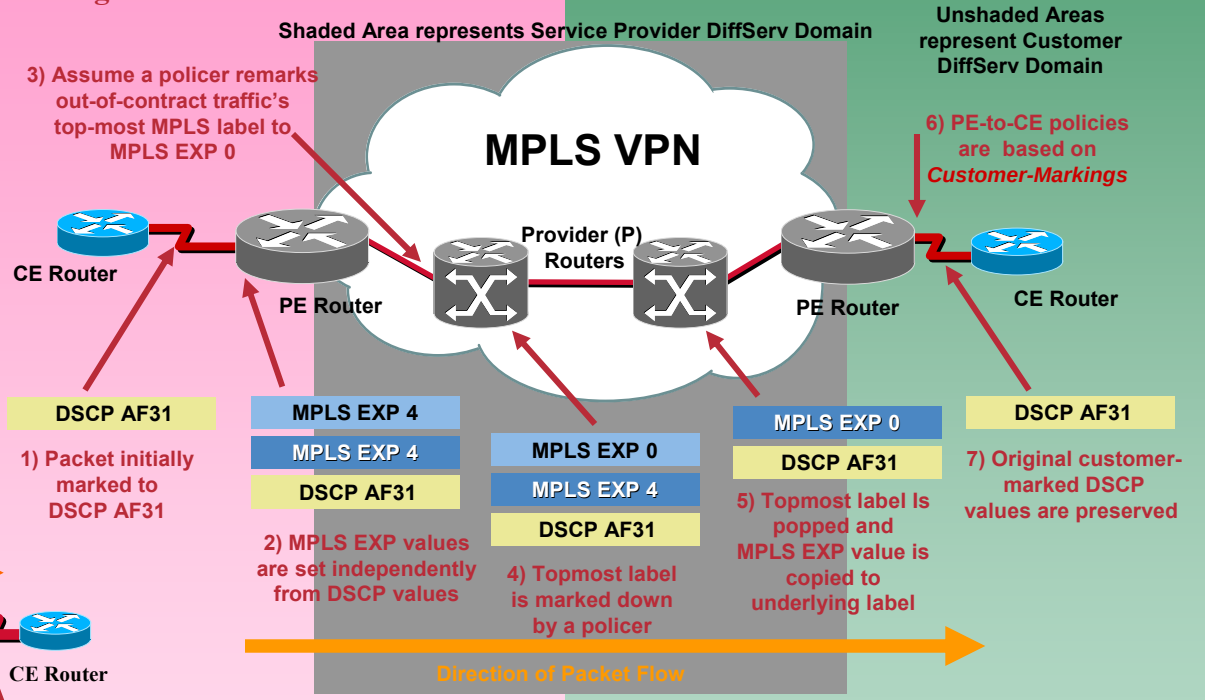


In order to guarantee end-to-end QoS, enterprises must co-manage QoS with their MPLS VPN service providers; their policies must be both consistent and complementary.

Service providers can mark at Layer 2 (MPLS EXP) or at Layer 3 (DSCP).

RFC 3270 presents three modes of MPLS/DiffServ marking for service providers:

1) Uniform Mode: SP can remark customer DSCP values
2) Pipe Mode: SP does not remark customer DSCP values (SP uses independent MPLS EXP markings); final PE-to-CE policies are based on *service provider's* markings
3) Short Pipe Mode (shown below): SP does not remark customer DSCP values (SP uses independent MPLS EXP markings); final PE-to-CE policies are based on *customer's* markings



Service providers can guarantee service levels within their core by:

1) Aggregate Bandwidth Overprovisioning: adding redundant links when utilization hits 50% (simple to implement, but expensive and inefficient)
2) Core DiffServ policies: simplified DiffServ policies for core links
3) MPLS TE: TE provides granular policy-based control over traffic flows within the core

szigeti@cisco.com 2004

QoS Design for IPSec VPNs

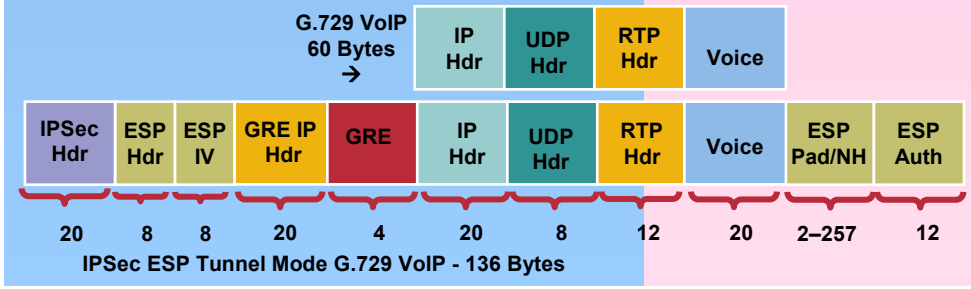
IPSec VPNs achieve network segregation and privacy via encryption. IPSec VPNs are built by overlaying a point-to-point mesh over the Internet using Layer 3-encrypted tunnels. Encryption/ decryption is performed at these tunnel endpoints and the protected traffic is carried across the shared network.

Three main QoS considerations specific to IPSec VPNs are:
1) the additional bandwidth required by IPSec encryption and authentication,
2) the marginal time element required at each point where encryption/decryption takes place
3) Anti-Replay interactions

1) IPSec Bandwidth Overhead

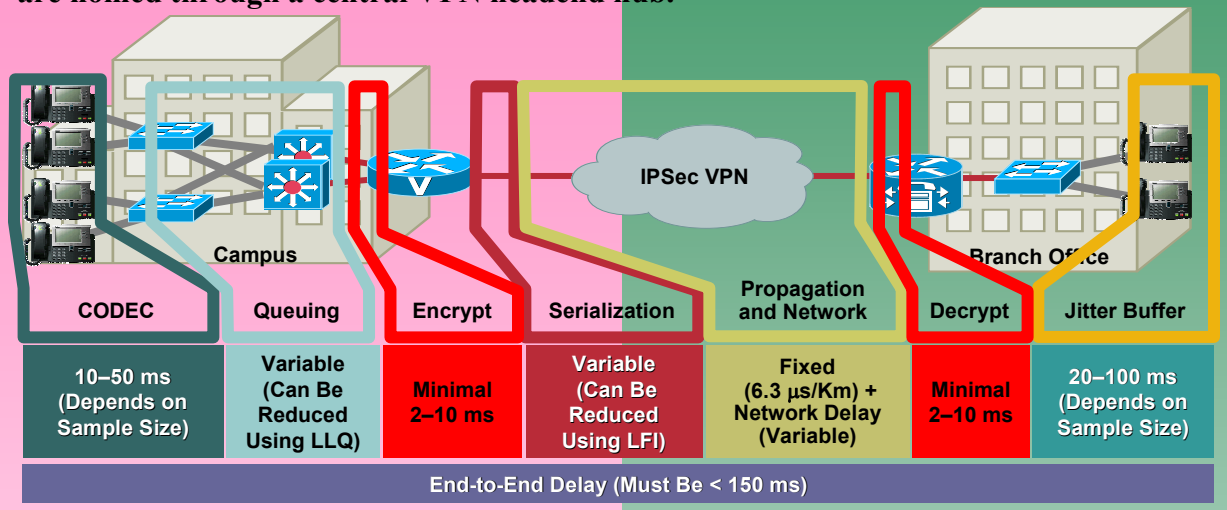
The additional bandwidth required to encrypt and authenticate a packet needs to be factored into account when provisioning QoS policies.

This is especially important for VoIP, where IPSec could more than double the size of a G.729 voice packet, as shown below.



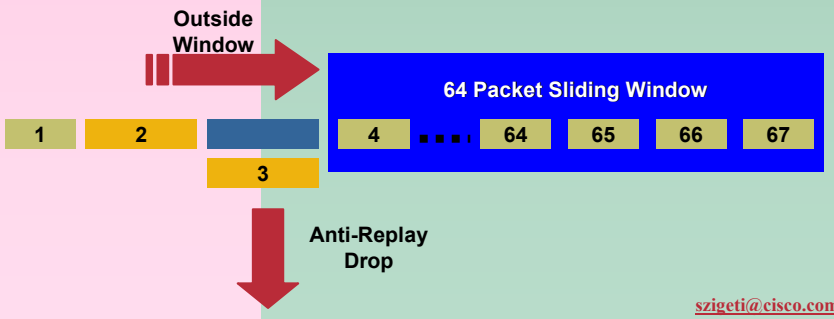
2) Encryption/Decryption Delays

A marginal time element for encryption and decryption should be factored into the end-to-end delay budget for realtime applications, such as VoIP. Typically these processes require 2-10 ms per hop, but may be doubled in the case of spoke-to-spoke VoIP calls that are homed through a central VPN headend hub.



3) Anti-Replay Interactions

Anti-Relay is a standards-defined mechanism to protect IPSec VPNs from hackers. If packets arrive outside of a 64-byte window, then they are considered hacked and are dropped prior to decryption. QoS queuing policies may re-order packets such that they fall outside of the Anti-Replay window. Therefore, IPSec VPN QoS policies need to be properly tuned to minimize Anti-Replay drops.



szigeti@cisco.com 2004

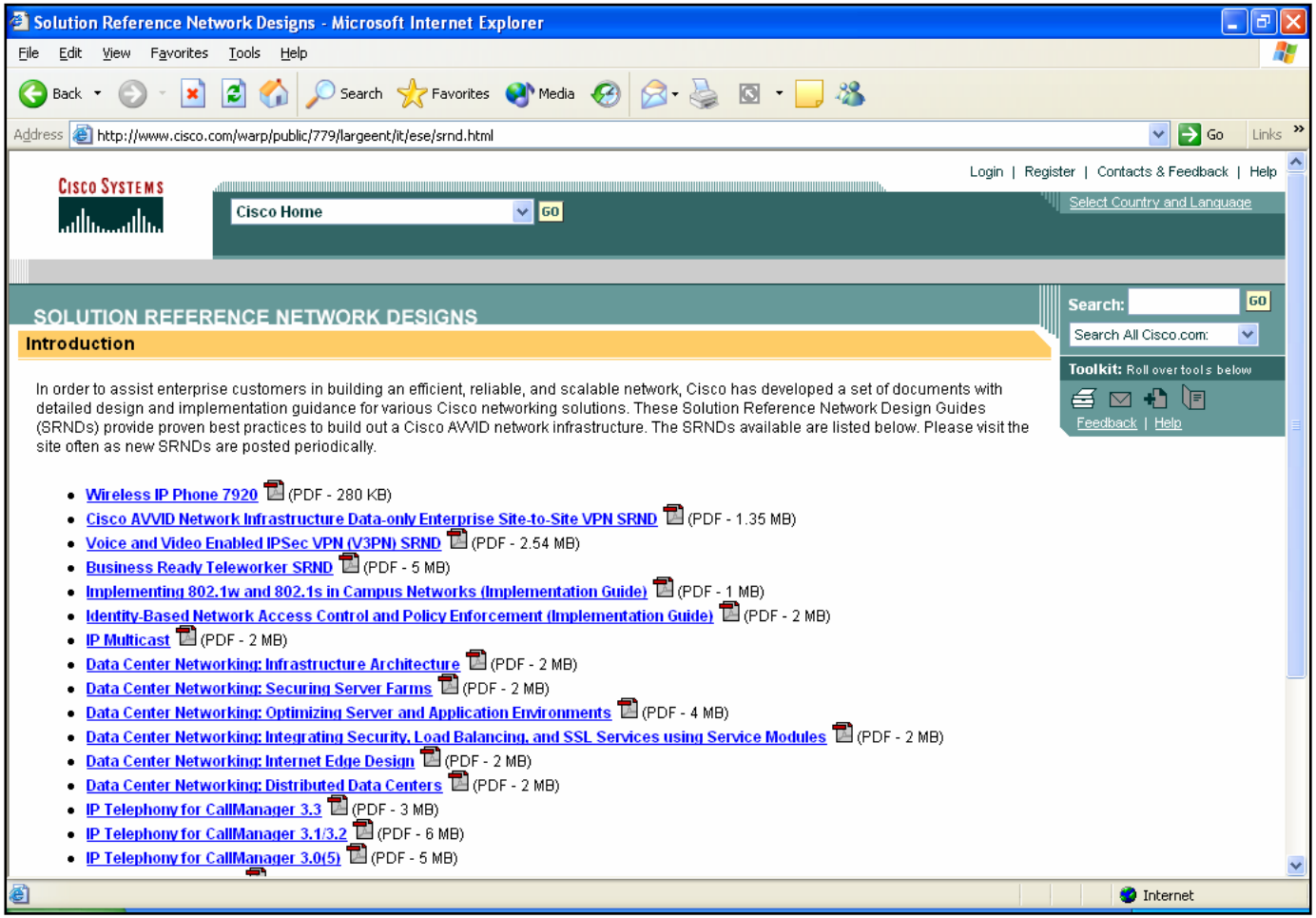
Q & A

REFERENCES

Solution Reference Network Design Guides
Enterprise QoS Design Guide

Cisco.com

http://www.cisco.com/go/srnd

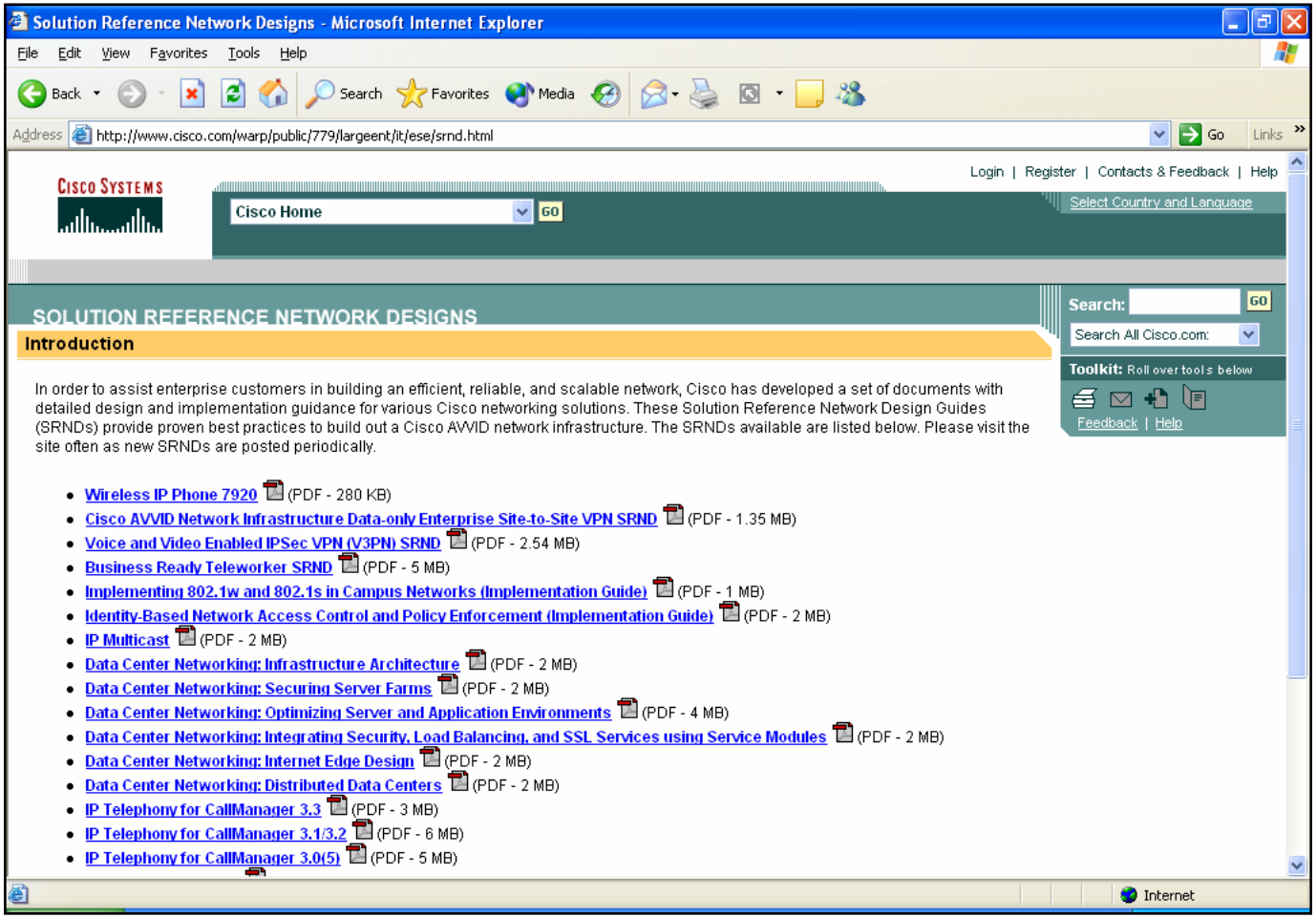


Solution Reference Network Design Guides

Site-to-Site V³PN Design Guide

Cisco.com

http://www.cisco.com/go/srnd

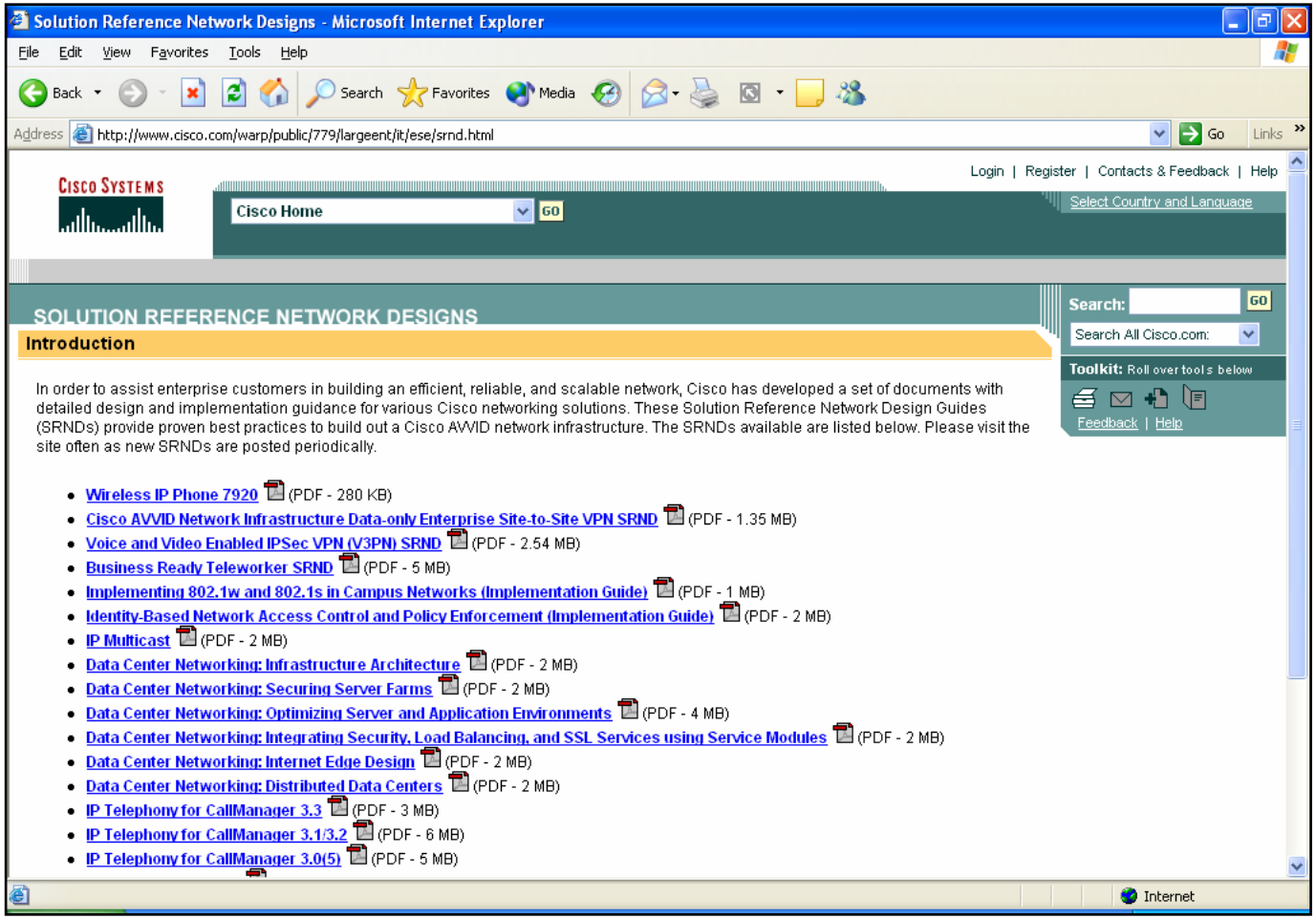


Solution Reference Network Design Guides

Teleworker V³PN Design Guide

Cisco.com

http://www.cisco.com/go/srnd

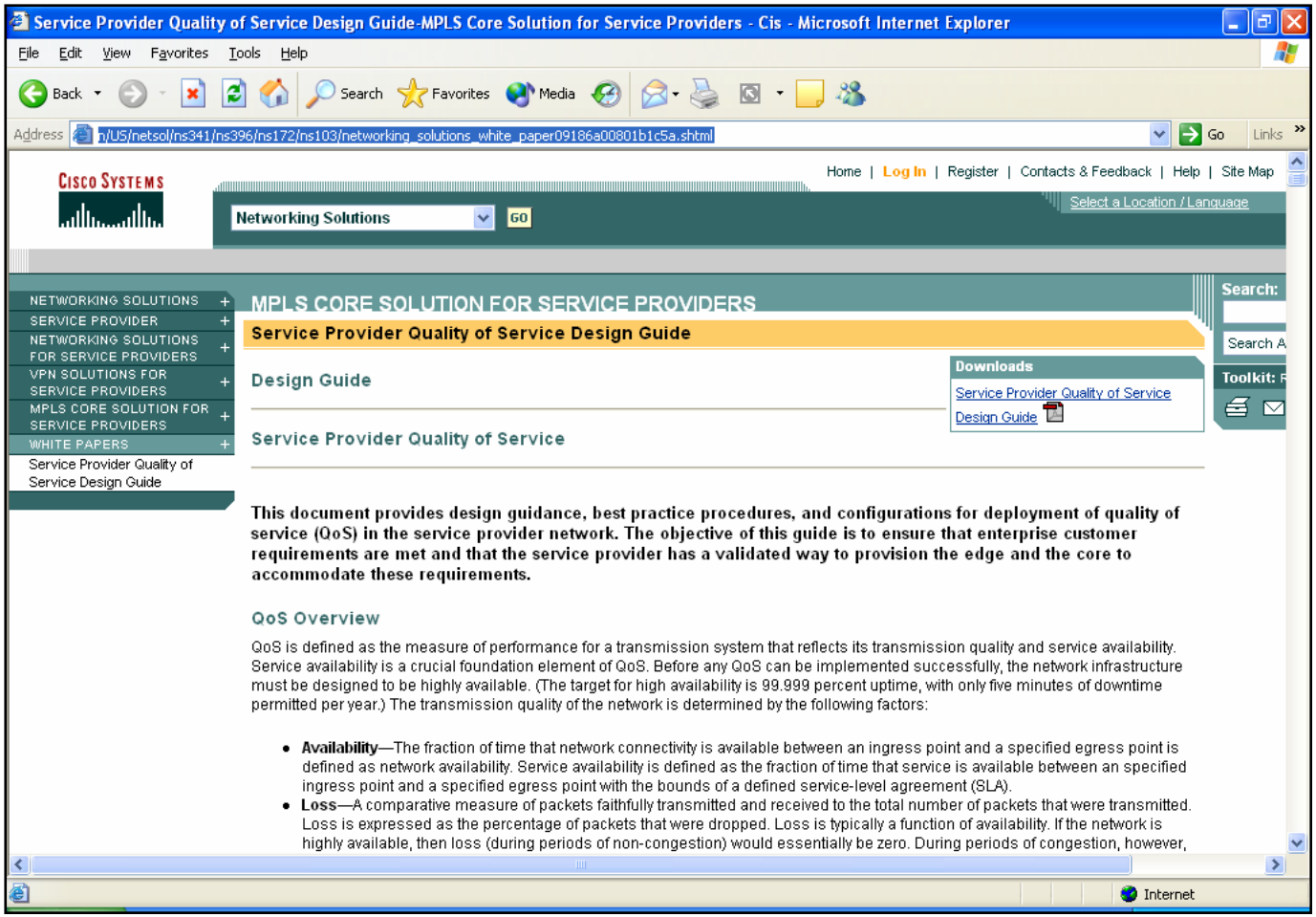


Solution Reference Network Design Guides

Service Provider QoS Design (MPLS VPNs)

Cisco.com

http://www.cisco.com/en/US/netsol/ns341/ns396/ns172/ns103/networking_solutions_white_paper09186a00801b1c5a.shtml



Reference Materials
DiffServ Standards

Cisco.com

- RFC 2474 “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”
  http://www.ietf.org/rfc/rfc2474
- RFC 2475 “An Architecture for Differentiated Services”
  http://www.ietf.org/rfc/rfc2475
- RFC 2597 “Assured Forwarding PHB Group”
  http://www.ietf.org/rfc/rfc2597
- RFC 2697 “A Single Rate Three Color Marker”
  http://www.ietf.org/rfc/rfc2697
- RFC 2698 “A Two Rate Three Color Marker”
  http://www.ietf.org/rfc/rfc2698
- RFC 3246 “An Expedited Forwarding PHB (Per-Hop Behavior)”
  http://www.ietf.org/rfc/rfc3246

Reference Materials
Campus QoS Documentation

Cisco.com

- **Cisco Catalyst 2950 QoS**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/12120ea2/2950scg/swqos.htm
- **Cisco Catalyst 2970 QoS**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2970/12220se/2970scg/swqos.htm
- **Cisco Catalyst 3550 QoS**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/12120ea2/3550scg/swqos.htm
- **Cisco Catalyst 3750 QoS**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12220se/3750scg/swqos.htm
- **Cisco Catalyst 4500 (Cisco IOS) QoS**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_2_18/config/qos.htm
- **Cisco Catalyst 6500 (Cisco Catalyst OS)**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_3/confg_gd/qos.htm
- **Cisco Catalyst 6500 (Cisco IOS)**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm

Reference Materials
WAN/Branch Cisco IOS QoS Documentation

Cisco.com

- **Classification Tools**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/qos_vcg.htm#1000913
- **Congestion Management (Queuing) Tools**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/qos_vcg.htm#1001619
- **Congestion Avoidance (Selective Dropping) Tools**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/qos_vcg.htm#1000448
- **Policing and Shaping Tools**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/qos_vcg.htm#1001018
- **Link-Specific Tools**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/qos_vcg.htm#1001728
- **Modular QoS CLI (MQC) Syntax**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/qos_vcg.htm#1001811

Reference Materials
NBAR vs. Worms (SAFE White Papers)

- **Code Red**
  http://www.cisco.com/en/US/products/hw/routers/ps359/products_tech_note09186a00800fc176.shtml
- **Nimda**
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a0080110d17.shtml
- **SQL Slammer**
  http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801cd7f5.shtml
- **DCOM/W32/Blaster**
  http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801b2391.shtml
- **Sasser**
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns441/c664/cdccont_0900aecd800f613b.pdf
- **NBAR Custom PDLM (Cisco IOS 12.3(4)T Documentation)**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

Reference Materials
MPLS VPN Standards

Cisco.com

- RFC 2547 “BGP/MPLS VPNs”
  http://www.ietf.org/rfc/rfc2547
- RFC 2702 “Requirements for Traffic Engineering Over MPLS”
  http://www.ietf.org/rfc/rfc2702
- RFC 2917 “A Core MPLS IP VPN Architecture”
  http://www.ietf.org/rfc/rfc2917
- RFC 3270 “Multi-Protocol Label Switching (MPLS) Support of Differentiated Services”
  http://www.ietf.org/rfc/rfc3270
- RFC 3564 “Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering”
  http://www.ietf.org/rfc/rfc3564

Reference Materials
MPLS VPN QoS Documentation

Cisco.com

- **Configuring Multiprotocol Label Switching**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/xcftagc.htm
- **Configuring MPLS VPNs**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvpn13.htm
- **Configuring MPLS DiffServ Tunneling Modes**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftdtmode.htm
- **Configuring MPLS Traffic Engineering (MPLS TE)**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftbwadjm.htm
- **Configuring DiffServ-aware MPLS Traffic Engineering (MPLS DS-TE)**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_ds_te.htm

Reference Materials
AutoQoS Documentation

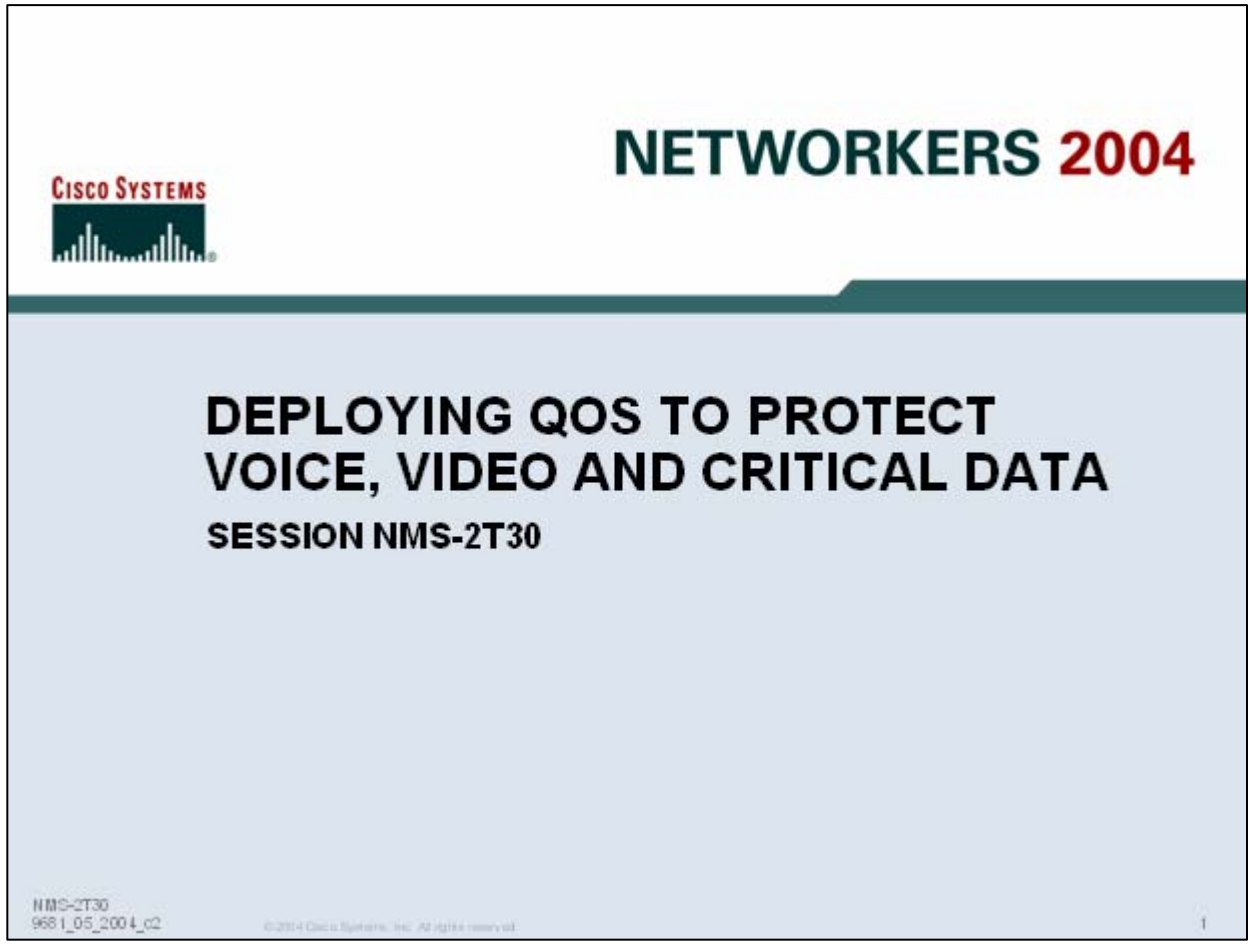
Cisco.com

- **AutoQoS VoIP for the Cisco Catalyst 2950**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/12120ea2/2950scg/swqos.htm#wp1125412
- **AutoQoS VoIP for the Cisco Catalyst 2970**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2970/12220se/2970scg/swqos.htm#wp1231112
- **AutoQoS VoIP for the Cisco Catalyst 3550**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/12120ea2/3550scg/swqos.htm#wp1185065
- **AutoQoS VoIP for the Cisco Catalyst 3750**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12220se/3750scg/swqos.htm#wp1231112
- **AutoQoS VoIP for the Cisco Catalyst 4550**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_2_18/config/qos.htm#1281380
- **AutoQoS VoIP for the Cisco Catalyst 6500 (Cisco Catalyst OS)**
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_3/confg_gd/autoqos.htm
- **AutoQoS VoIP for Cisco IOS Routers (Cisco IOS 12.2(15)T)**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftautoq1.htm
- **AutoQoS Enterprise for Cisco IOS Routers (Cisco IOS 12.3(7)T)**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/ftautoq2.htm

Reference Materials
Networkers QoS Design Techtorial

Cisco.com

ftp://ftpeng.cisco.com/szigeti/NW2004



9-hr Techtorial (450 slides)
Detailed designs and configs

LAN
- **Catalyst 2950**
- **Catalyst 3550**
- **Catalyst 2970/3750**
- **Catalyst 4500**
- **Catalyst 6500**

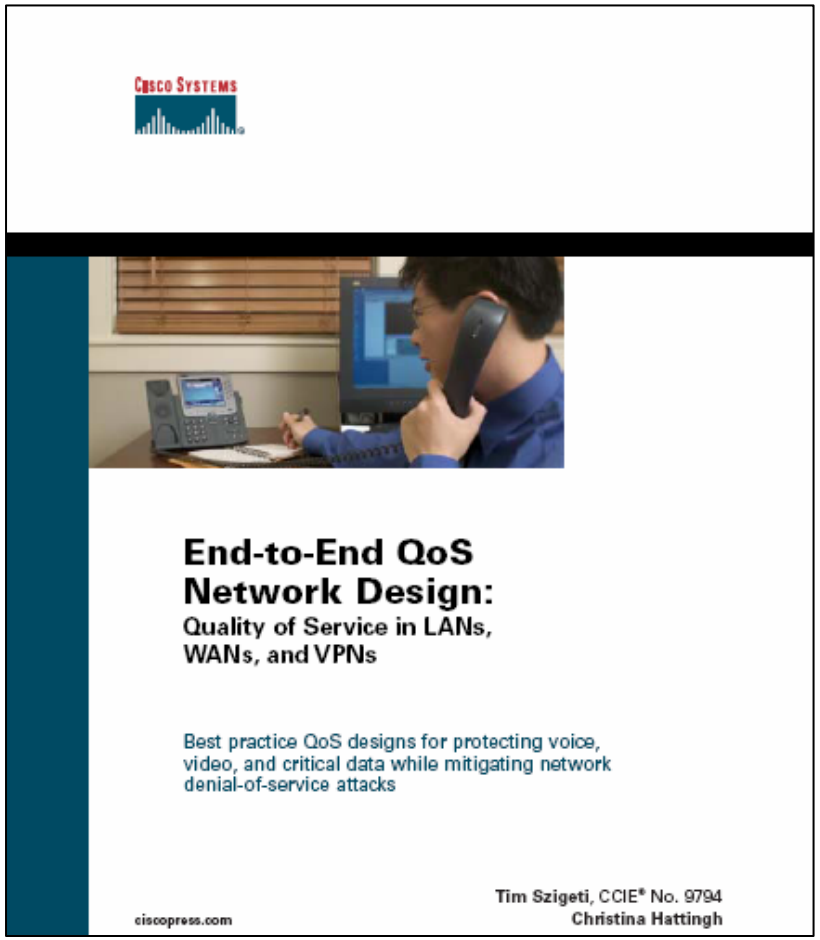
WAN/Branch
- **Leased Lines**
- **Frame Relay**
- **ATM**
- **ATM-to-FR SIW**
- **ISDN**
- **NBAR for Worm Policing**

VPN
- **MPLS**
- **IPSec (Site-to-Site)**
- **IPSec (Teleworker)**

Reference Materials

Cisco Press Book: End-to-End QoS Design

http://www.ciscopress.com/title/1587051761



ISBN: 1587051761
Publish Date: Nov 9/04

LAN
- **Catalyst 2950**
- **Catalyst 3550**
- **Catalyst 2970/3560/3750**
- **Catalyst 4500**
- **Catalyst 6500**

WAN/Branch
- **Leased Lines**
- **Frame Relay**
- **ATM**
- **ATM-to-FR SIW**
- **ISDN**
- **NBAR for Worm Policing**

VPN
- **MPLS (for Enterprise Subscribers)**
- **MPLS (for Service Providers)**
- **IPSec (Site-to-Site)**
- **IPSec (Teleworker)**